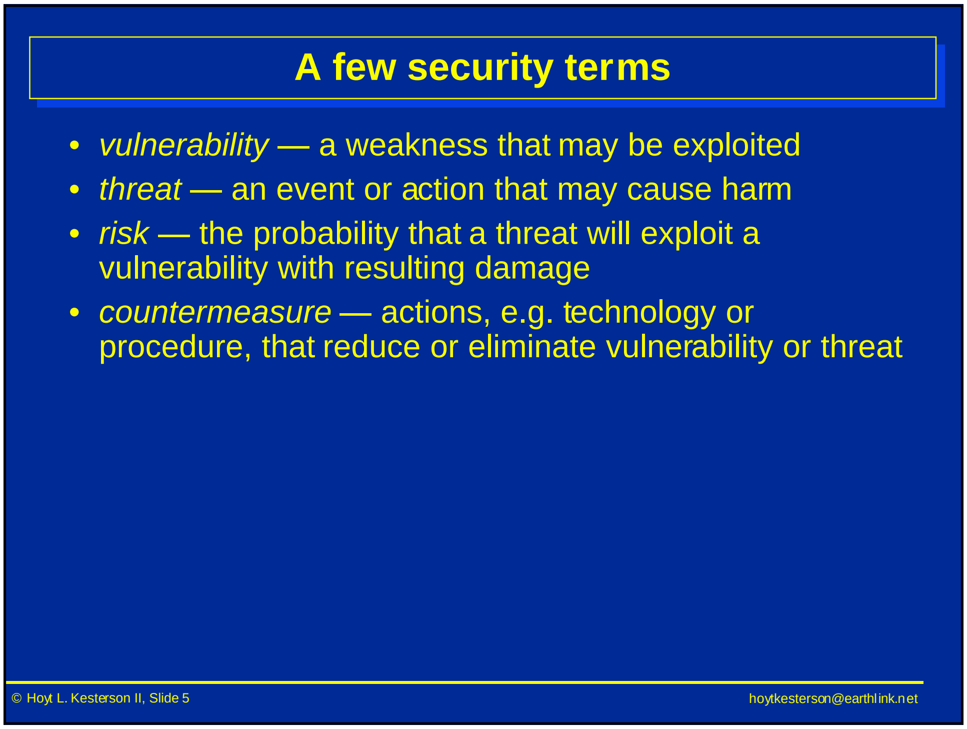
Securing Your Enterprise

Security Techno-Babble 101

Hoyt L. Kesterson II

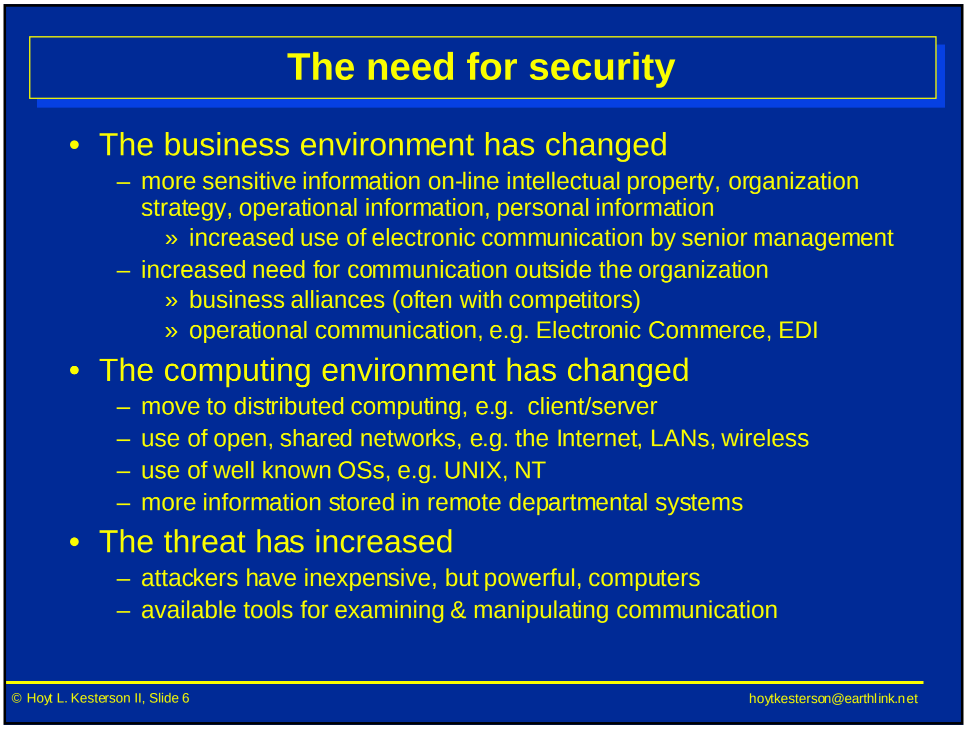
hoytkesterson@Earthlink.net



A few security terms

- *vulnerability* — a weakness that may be exploited
- *threat* — an event or action that may cause harm
- *risk* — the probability that a threat will exploit a vulnerability with resulting damage
- *countermeasure* — actions, e.g. technology or procedure, that reduce or eliminate vulnerability or threat

© Hoyt L. Kesterson II, Slide 5 hoytkesterson@earthlink.net



The need for security

- The business environment has changed
  - more sensitive information on-line intellectual property, organization strategy, operational information, personal information
    - » increased use of electronic communication by senior management
  - increased need for communication outside the organization
    - » business alliances (often with competitors)
    - » operational communication, e.g. Electronic Commerce, EDI
- The computing environment has changed
  - move to distributed computing, e.g. client/server
  - use of open, shared networks, e.g. the Internet, LANs, wireless
  - use of well known OSs, e.g. UNIX, NT
  - more information stored in remote departmental systems
- The threat has increased
  - attackers have inexpensive, but powerful, computers
  - available tools for examining & manipulating communication

© Hoyt L. Kesterson II, Slide 6 hoytkesterson@earthlink.net

IOU
~~$100~~
$1000

The threats

Line taps (sniffing)
Masquerades
Message alteration
Message replay
Unauthorized access to resources
Denial of Service

© Hoyt L. Kesterson II, Slide 7 hoytkesterson@earthlink.net

The LAN—an old–fashioned party line

© Hoyt L. Kesterson II, Slide 8

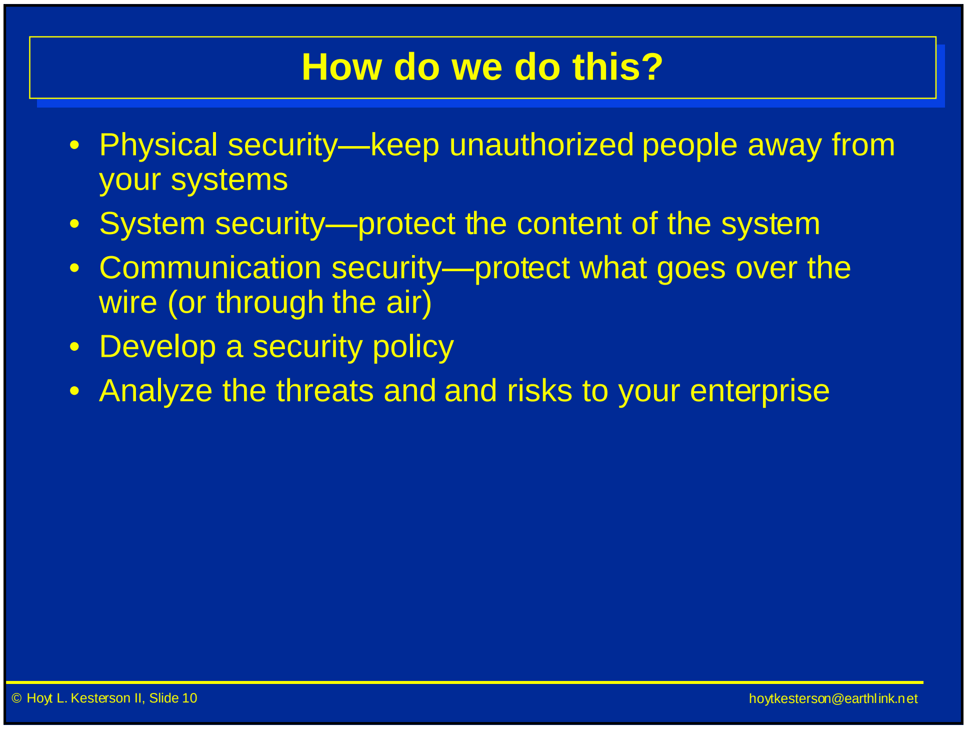
hoytkesterson@earthlink.net

The security countermeasures

- Is this the party to whom I am speaking?—authentication
  - —don't increase logon complexity; do single logon
- Allow me to trust electronic documents—digital signature
- Don't let unauthorized people change my stuff—integrity
- Don't let unauthorized people see my stuff—confidentiality
- Don't let them do it and say they didn't—non-repudiation
- Don't let them stop my work—avoid denial of service
- Don't make me hire a bunch of people to do this—administration & audit

© Hoyt L. Kesterson II, Slide 9

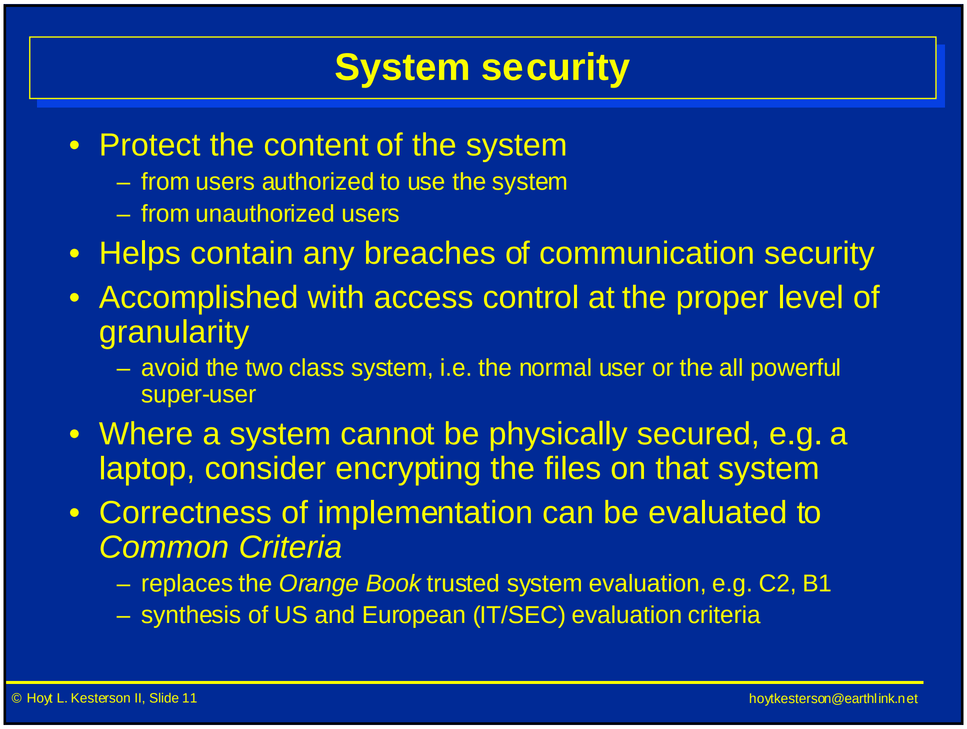
hoytkesterson@earthlink.net



How do we do this?

- Physical security—keep unauthorized people away from your systems
- System security—protect the content of the system
- Communication security—protect what goes over the wire (or through the air)
- Develop a security policy
- Analyze the threats and and risks to your enterprise

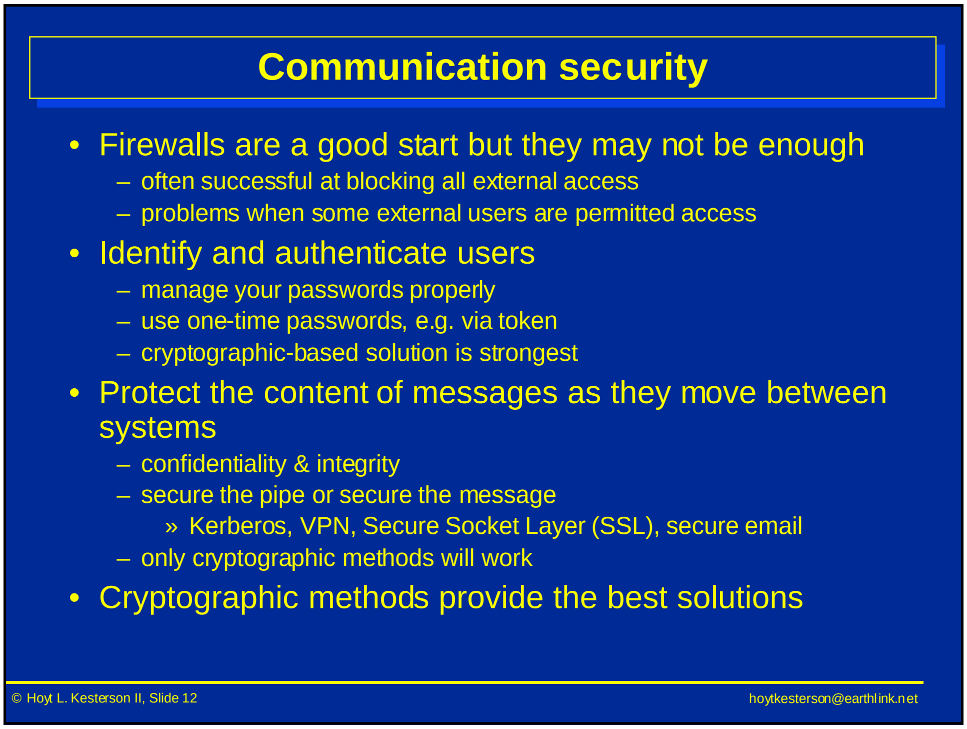
© Hoyt L. Kesterson II, Slide 10 hoytkesterson@earthlink.net



System security

- Protect the content of the system
  - from users authorized to use the system
  - from unauthorized users
- Helps contain any breaches of communication security
- Accomplished with access control at the proper level of granularity
  - avoid the two class system, i.e. the normal user or the all powerful super-user
- Where a system cannot be physically secured, e.g. a laptop, consider encrypting the files on that system
- Correctness of implementation can be evaluated to *Common Criteria*
  - replaces the *Orange Book* trusted system evaluation, e.g. C2, B1
  - synthesis of US and European (IT/SEC) evaluation criteria

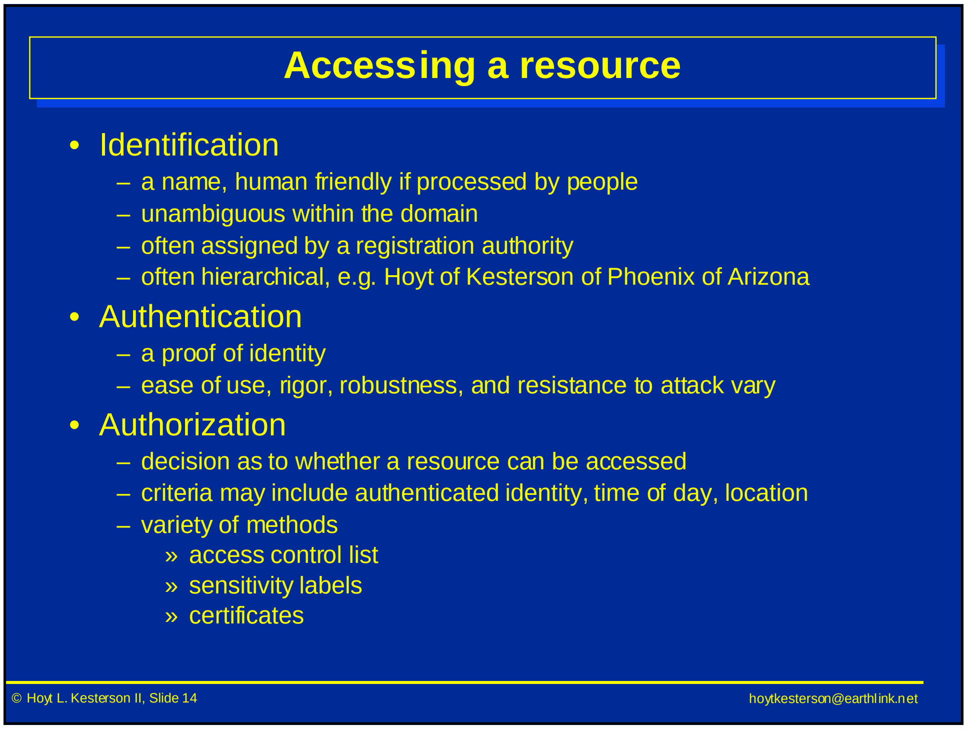
© Hoyt L. Kesterson II, Slide 11 hoytkesterson@earthlink.net



Communication security

- Firewalls are a good start but they may not be enough
  - often successful at blocking all external access
  - problems when some external users are permitted access
- Identify and authenticate users
  - manage your passwords properly
  - use one-time passwords, e.g. via token
  - cryptographic-based solution is strongest
- Protect the content of messages as they move between systems
  - confidentiality & integrity
  - secure the pipe or secure the message
    - » Kerberos, VPN, Secure Socket Layer (SSL), secure email
  - only cryptographic methods will work
- Cryptographic methods provide the best solutions

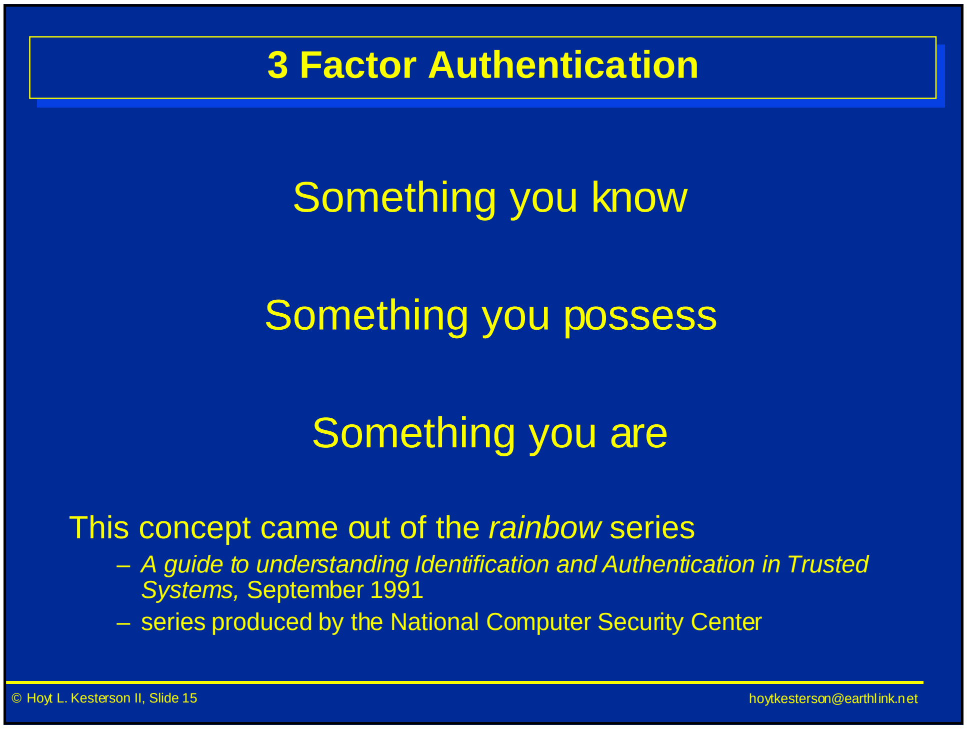
© Hoyt L. Kesterson II, Slide 12 hoytkesterson@earthlink.net



Accessing a resource

- Identification
  - a name, human friendly if processed by people
  - unambiguous within the domain
  - often assigned by a registration authority
  - often hierarchical, e.g. Hoyt of Kesterson of Phoenix of Arizona
- Authentication
  - a proof of identity
  - ease of use, rigor, robustness, and resistance to attack vary
- Authorization
  - decision as to whether a resource can be accessed
  - criteria may include authenticated identity, time of day, location
  - variety of methods
    - » access control list
    - » sensitivity labels
    - » certificates

© Hoyt L. Kesterson II, Slide 14 hoytkesterson@earthlink.net



3 Factor Authentication

Something you know

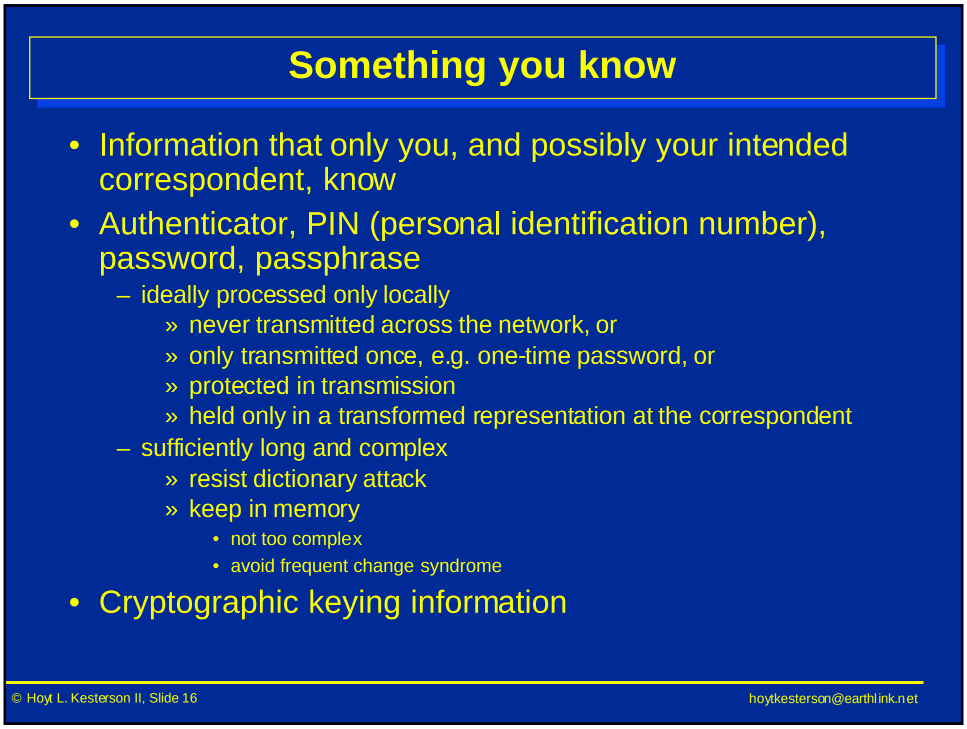
Something you possess

Something you are

This concept came out of the *rainbow* series

- *A guide to understanding Identification and Authentication in Trusted Systems,* September 1991
- series produced by the National Computer Security Center

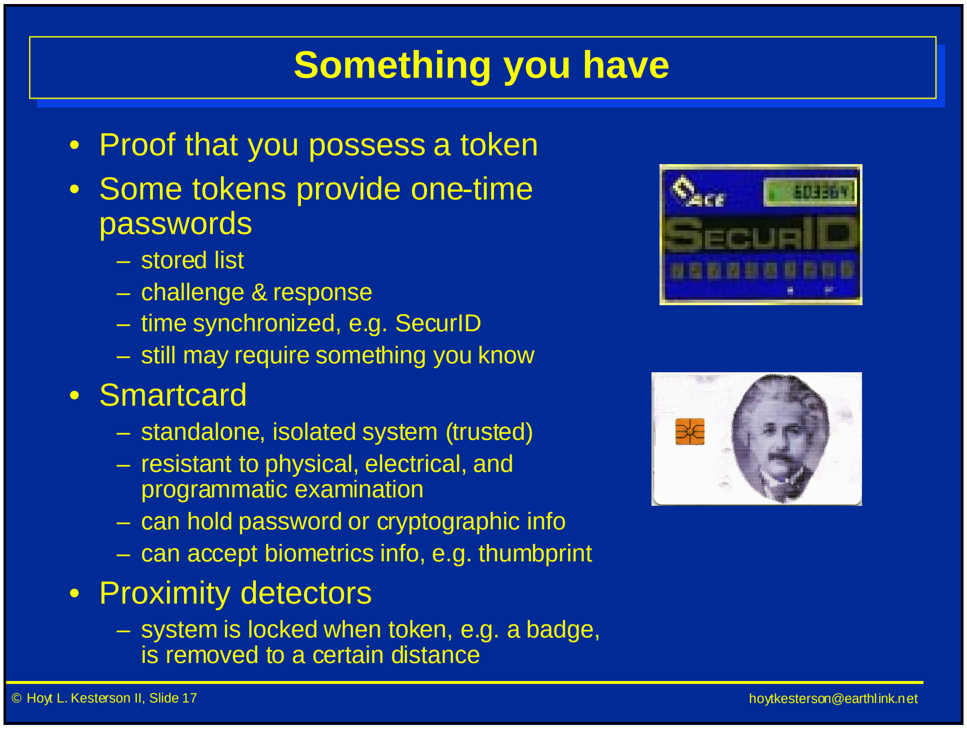
© Hoyt L. Kesterson II, Slide 15 hoytkesterson@earthlink.net



Something you know

- Information that only you, and possibly your intended correspondent, know
- Authenticator, PIN (personal identification number), password, passphrase
  - ideally processed only locally
    - never transmitted across the network, or
    - only transmitted once, e.g. one-time password, or
    - protected in transmission
    - held only in a transformed representation at the correspondent
  - sufficiently long and complex
    - resist dictionary attack
    - keep in memory
      - not too complex
      - avoid frequent change syndrome
- Cryptographic keying information

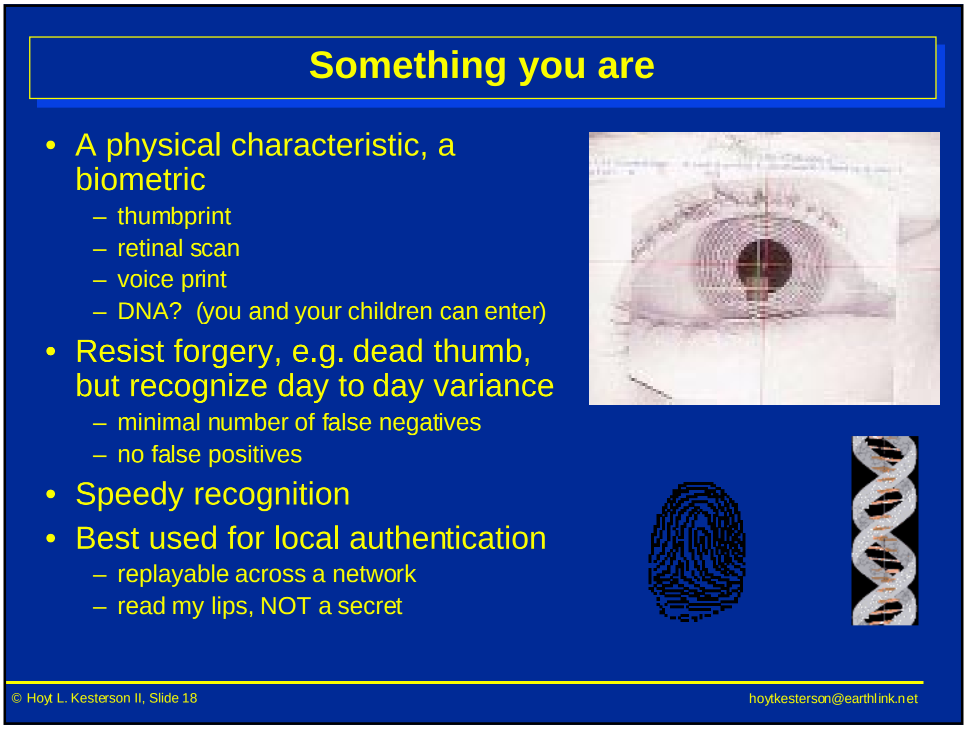
© Hoyt L. Kesterson II, Slide 16 hoytkesterson@earthlink.net



Something you have

- Proof that you possess a token
- Some tokens provide one-time passwords
  - stored list
  - challenge & response
  - time synchronized, e.g. SecurID
  - still may require something you know
- Smartcard
  - standalone, isolated system (trusted)
  - resistant to physical, electrical, and programmatic examination
  - can hold password or cryptographic info
  - can accept biometrics info, e.g. thumbprint
- Proximity detectors
  - system is locked when token, e.g. a badge, is removed to a certain distance

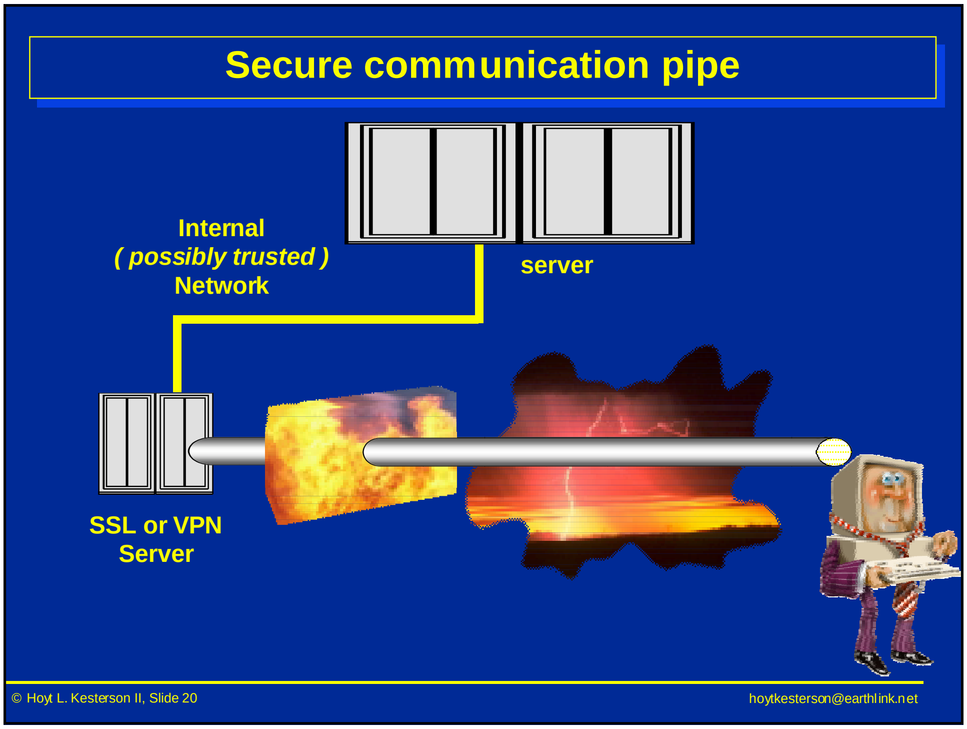
© Hoyt L. Kesterson II, Slide 17 hoytkesterson@earthlink.net



Something you are

- A physical characteristic, a biometric
  - thumbprint
  - retinal scan
  - voice print
  - DNA? (you and your children can enter)
- Resist forgery, e.g. dead thumb, but recognize day to day variance
  - minimal number of false negatives
  - no false positives
- Speedy recognition
- Best used for local authentication
  - replayable across a network
  - read my lips, NOT a secret

© Hoyt L. Kesterson II, Slide 18 hoytkesterson@earthlink.net



Secure communication pipe

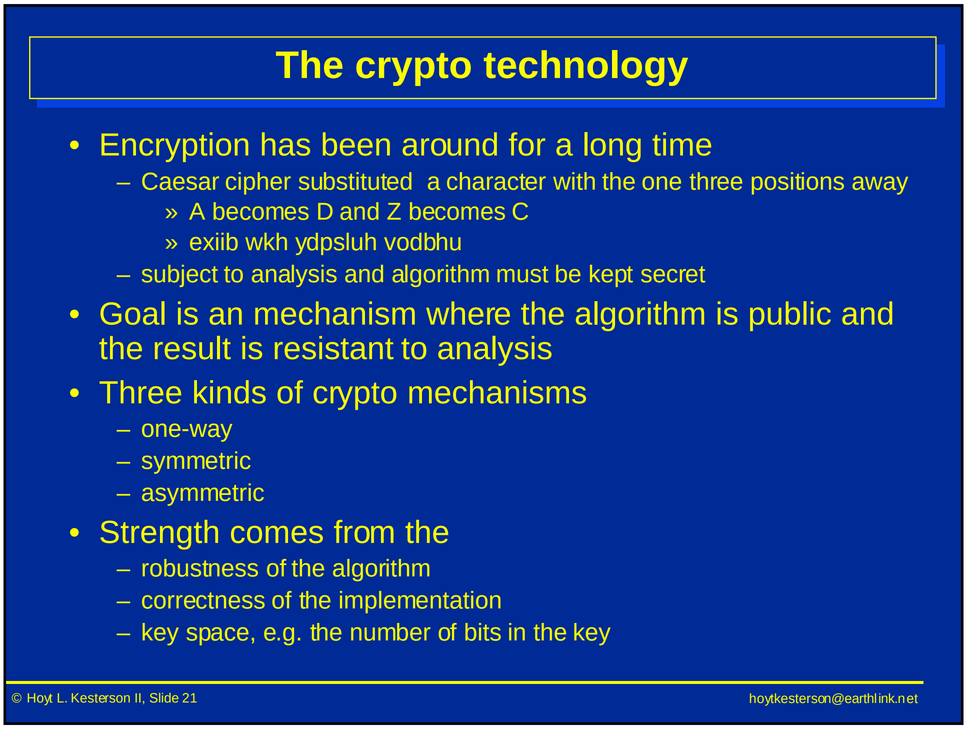
Internal
(possibly trusted)
Network

server

SSL or VPN
Server

© Hoyt L. Kesterson II, Slide 20

hoytkesterson@earthlink.net

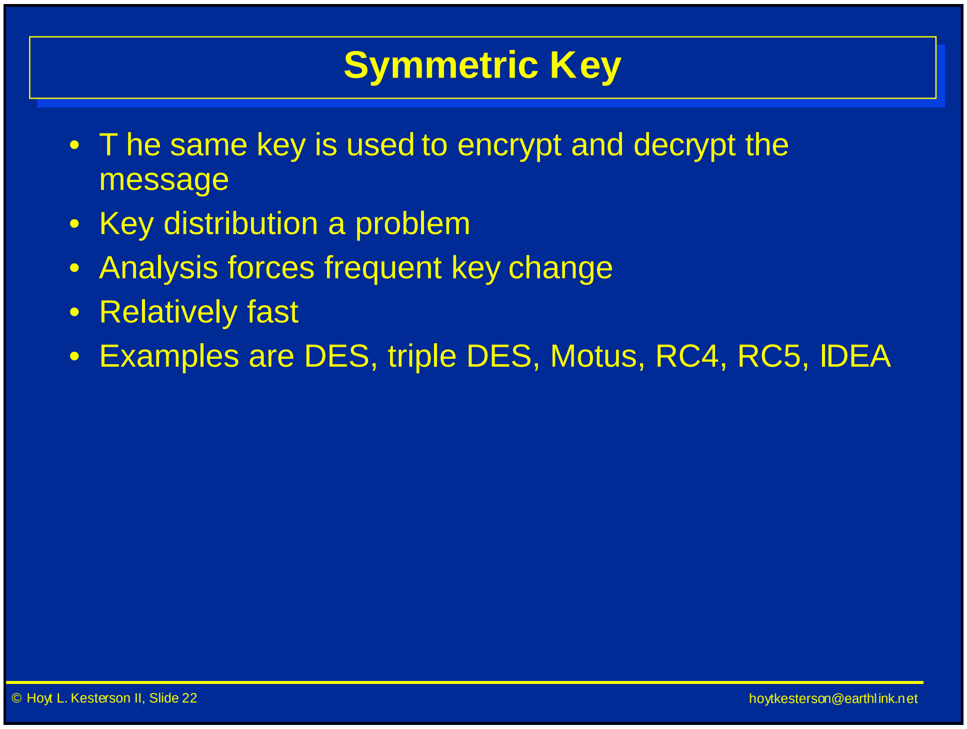


The crypto technology

- Encryption has been around for a long time
  - Caesar cipher substituted a character with the one three positions away
    - » A becomes D and Z becomes C
    - » exiib wkh ydpsluh vodbhu
  - subject to analysis and algorithm must be kept secret
- Goal is an mechanism where the algorithm is public and the result is resistant to analysis
- Three kinds of crypto mechanisms
  - one-way
  - symmetric
  - asymmetric
- Strength comes from the
  - robustness of the algorithm
  - correctness of the implementation
  - key space, e.g. the number of bits in the key

© Hoyt L. Kesterson II, Slide 21

hoytkesterson@earthlink.net

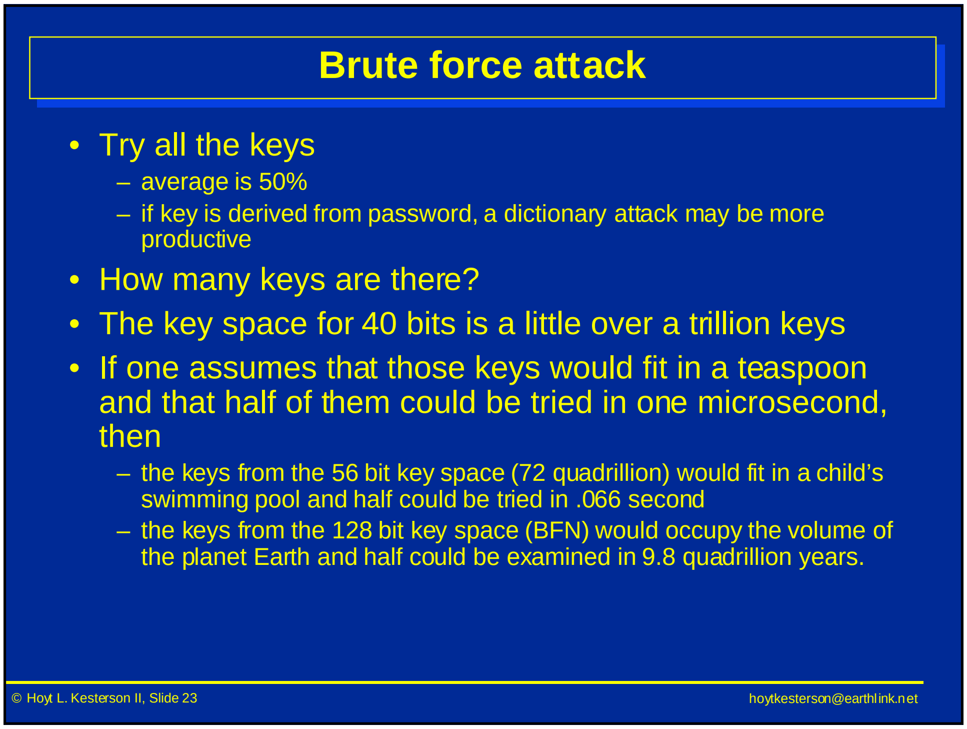


Symmetric Key

- T he same key is used to encrypt and decrypt the message
- Key distribution a problem
- Analysis forces frequent key change
- Relatively fast
- Examples are DES, triple DES, Motus, RC4, RC5, IDEA

© Hoyt L. Kesterson II, Slide 22

hoytkesterson@earthlink.net

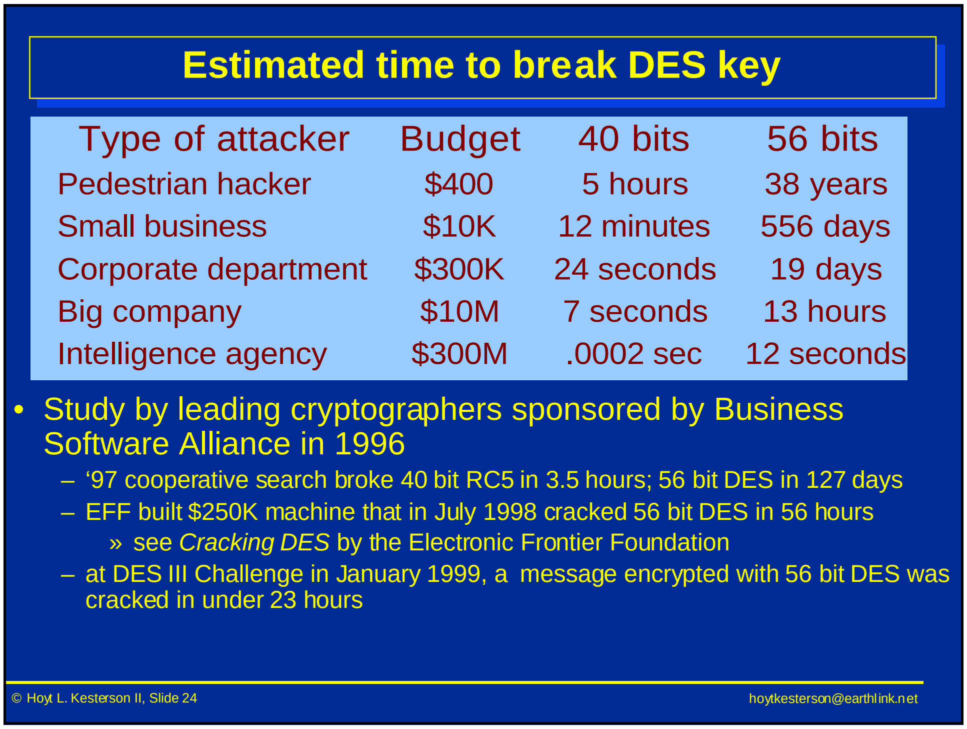


Brute force attack

- Try all the keys
  - average is 50%
  - if key is derived from password, a dictionary attack may be more productive
- How many keys are there?
- The key space for 40 bits is a little over a trillion keys
- If one assumes that those keys would fit in a teaspoon and that half of them could be tried in one microsecond, then
  - the keys from the 56 bit key space (72 quadrillion) would fit in a child’s swimming pool and half could be tried in .066 second
  - the keys from the 128 bit key space (BFN) would occupy the volume of the planet Earth and half could be examined in 9.8 quadrillion years.

© Hoyt L. Kesterson II, Slide 23

hoytkesterson@earthlink.net

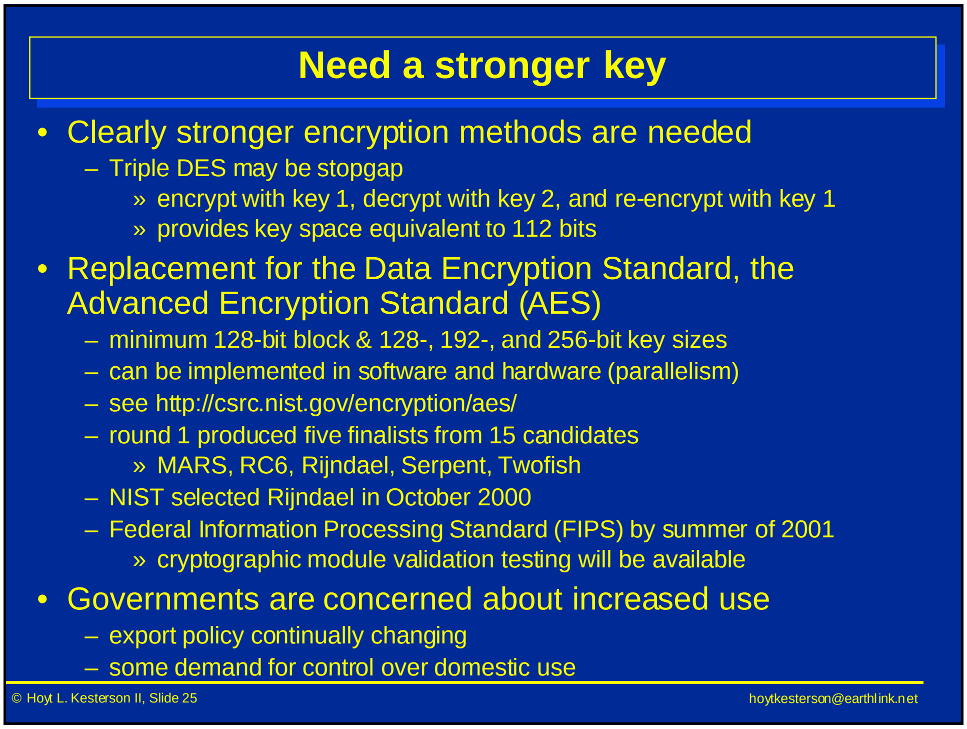


Estimated time to break DES key

Type of attacker	Budget	40 bits	56 bits
Pedestrian hacker	$400	5 hours	38 years
Small business	$10K	12 minutes	556 days
Corporate department	$300K	24 seconds	19 days
Big company	$10M	7 seconds	13 hours
Intelligence agency	$300M	.0002 sec	12 seconds

- Study by leading cryptographers sponsored by Business Software Alliance in 1996
  - '97 cooperative search broke 40 bit RC5 in 3.5 hours; 56 bit DES in 127 days
  - EFF built $250K machine that in July 1998 cracked 56 bit DES in 56 hours
    - see *Cracking DES* by the Electronic Frontier Foundation
  - at DES III Challenge in January 1999, a message encrypted with 56 bit DES was cracked in under 23 hours

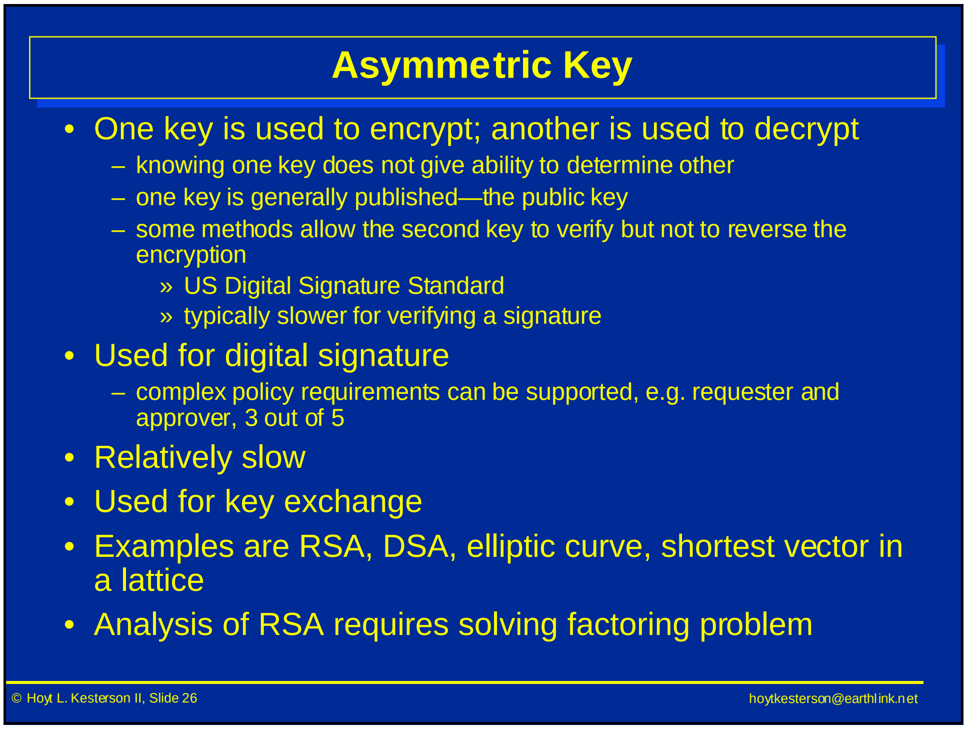
© Hoyt L. Kesterson II, Slide 24 hoytkesterson@earthlink.net



Need a stronger key

- Clearly stronger encryption methods are needed
  - Triple DES may be stopgap
    - encrypt with key 1, decrypt with key 2, and re-encrypt with key 1
    - provides key space equivalent to 112 bits
- Replacement for the Data Encryption Standard, the Advanced Encryption Standard (AES)
  - minimum 128-bit block & 128-, 192-, and 256-bit key sizes
  - can be implemented in software and hardware (parallelism)
  - see http://csrc.nist.gov/encryption/aes/
  - round 1 produced five finalists from 15 candidates
    - MARS, RC6, Rijndael, Serpent, Twofish
  - NIST selected Rijndael in October 2000
  - Federal Information Processing Standard (FIPS) by summer of 2001
    - cryptographic module validation testing will be available
- Governments are concerned about increased use
  - export policy continually changing
  - some demand for control over domestic use

© Hoyt L. Kesterson II, Slide 25 hoytkesterson@earthlink.net

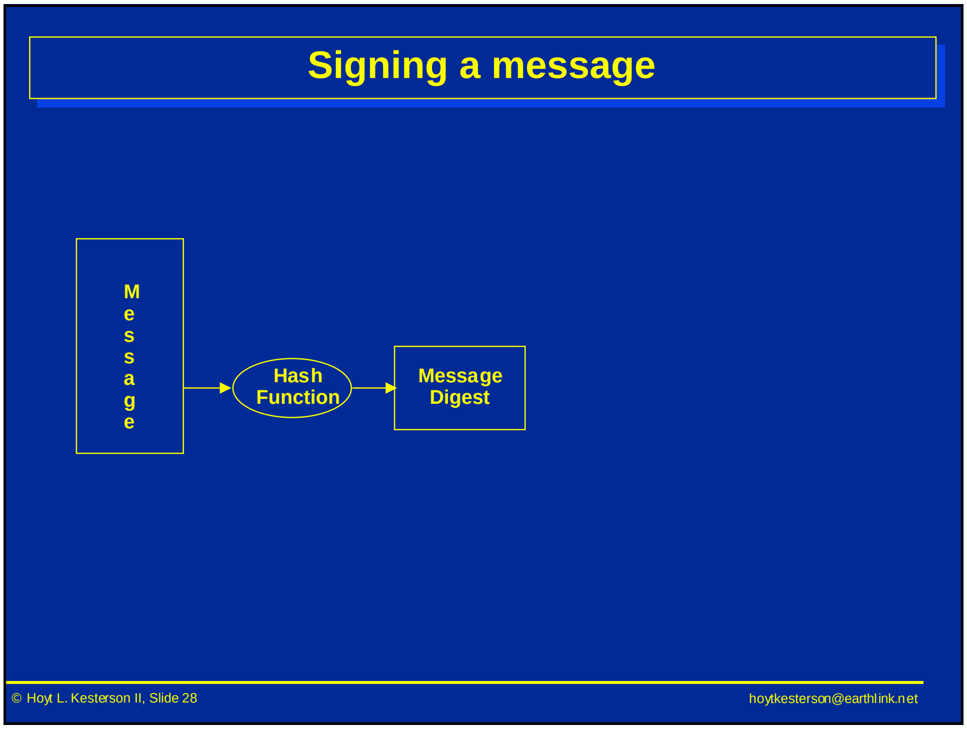


Asymmetric Key

- One key is used to encrypt; another is used to decrypt
  - knowing one key does not give ability to determine other
  - one key is generally published—the public key
  - some methods allow the second key to verify but not to reverse the encryption
    - US Digital Signature Standard
    - typically slower for verifying a signature
- Used for digital signature
  - complex policy requirements can be supported, e.g. requester and approver, 3 out of 5
- Relatively slow
- Used for key exchange
- Examples are RSA, DSA, elliptic curve, shortest vector in a lattice
- Analysis of RSA requires solving factoring problem

© Hoyt L. Kesterson II, Slide 26

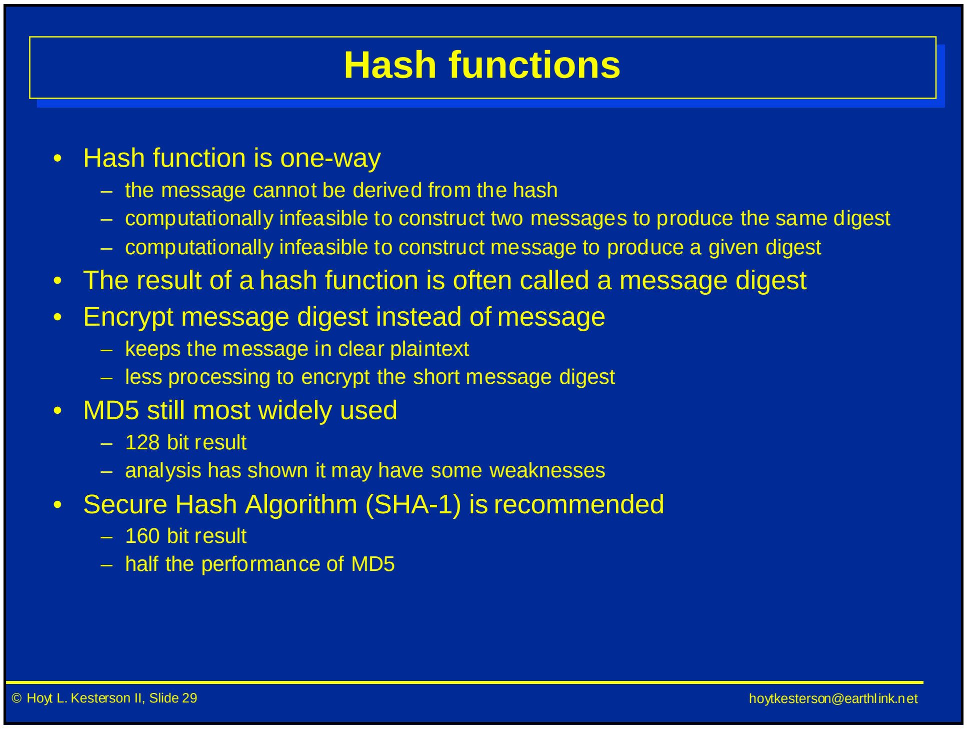
hoytkesterson@earthlink.net



Signing a message

© Hoyt L. Kesterson II, Slide 28

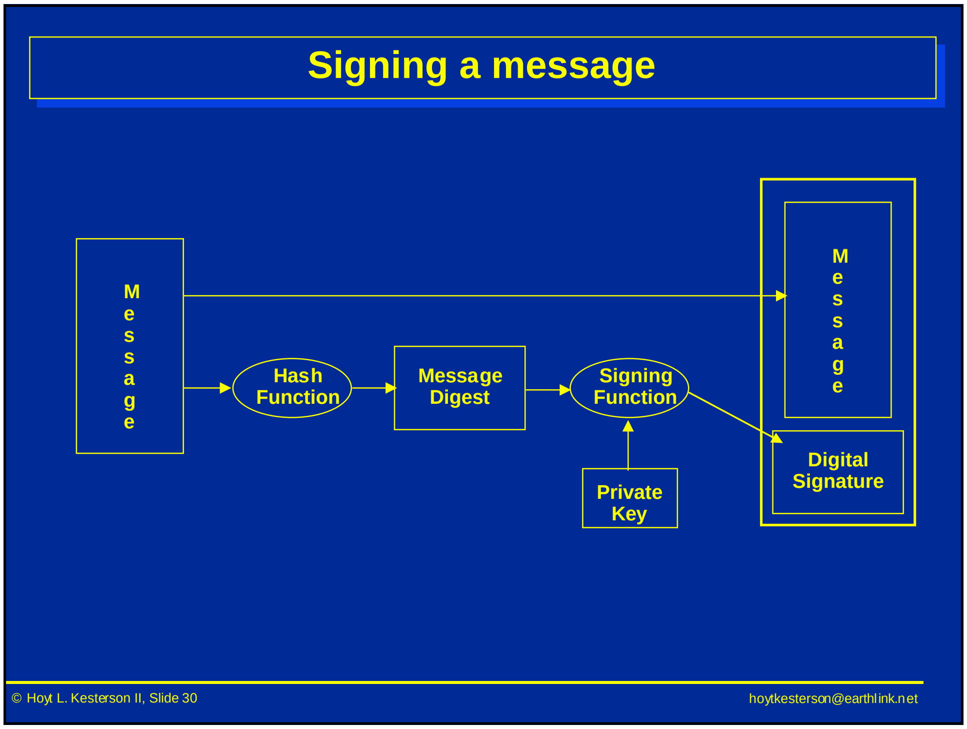
hoytkesterson@earthlink.net



Hash functions

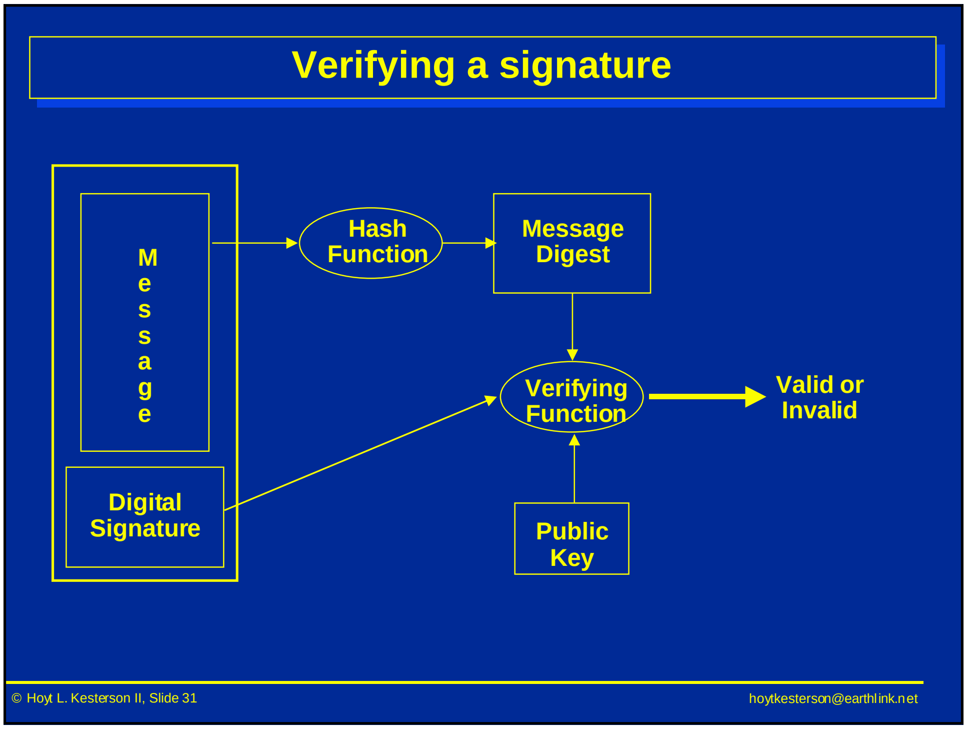
- Hash function is one-way
  - the message cannot be derived from the hash
  - computationally infeasible to construct two messages to produce the same digest
  - computationally infeasible to construct message to produce a given digest
- The result of a hash function is often called a message digest
- Encrypt message digest instead of message
  - keeps the message in clear plaintext
  - less processing to encrypt the short message digest
- MD5 still most widely used
  - 128 bit result
  - analysis has shown it may have some weaknesses
- Secure Hash Algorithm (SHA-1) is recommended
  - 160 bit result
  - half the performance of MD5

© Hoyt L. Kesterson II, Slide 29 hoytkesterson@earthlink.net



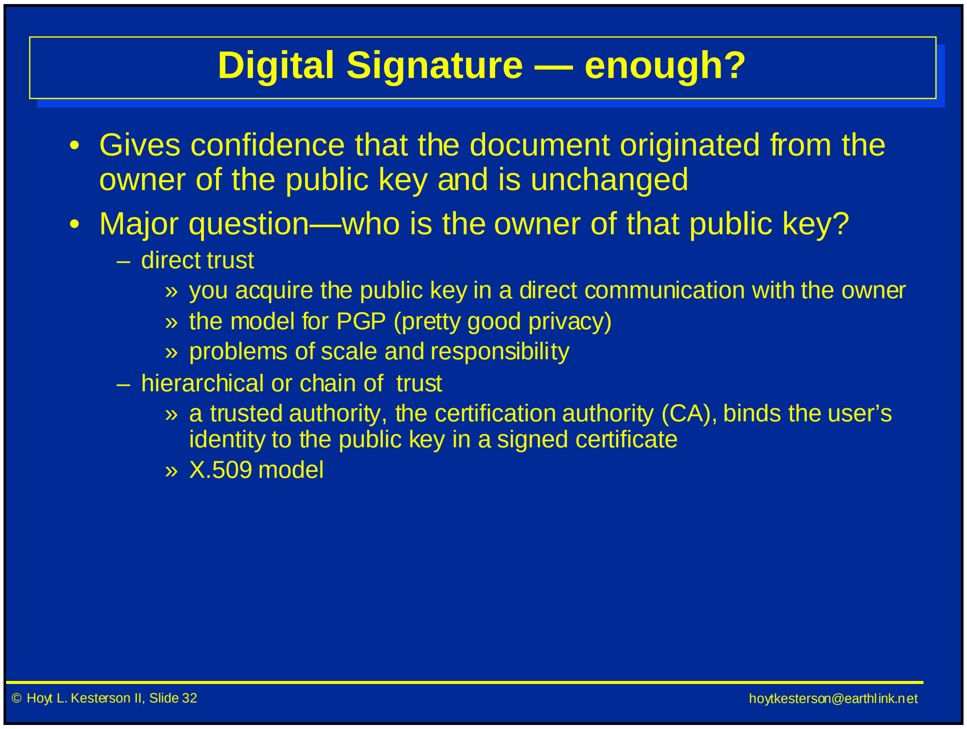
Signing a message

© Hoyt L. Kesterson II, Slide 30 hoytkesterson@earthlink.net



Verifying a signature

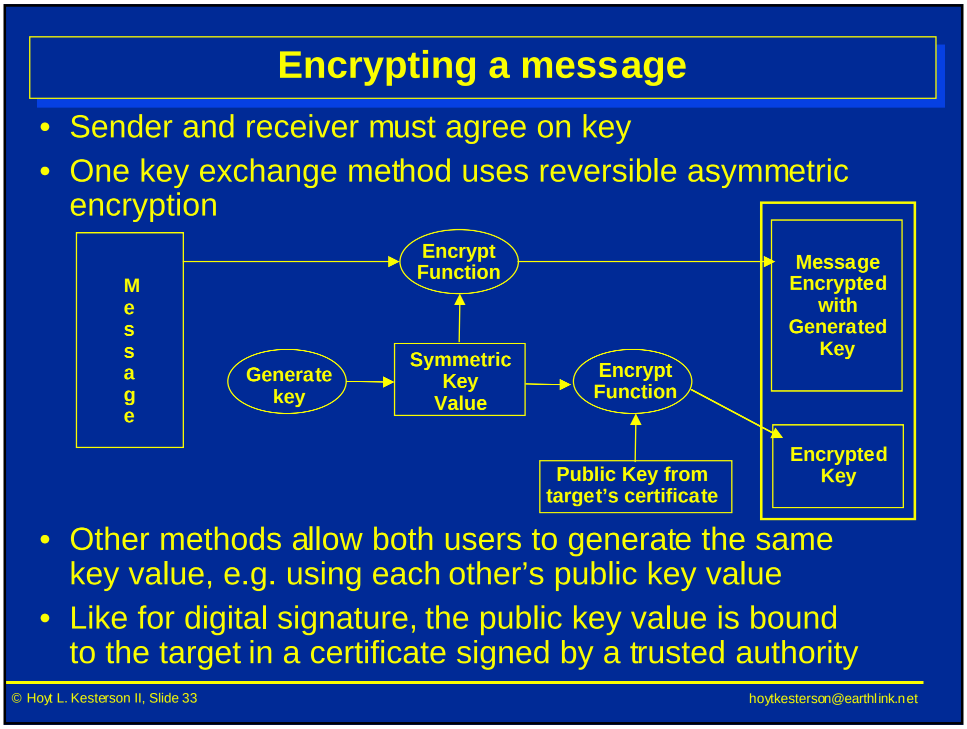
© Hoyt L. Kesterson II, Slide 31 hoytkesterson@earthlink.net



Digital Signature — enough?

- Gives confidence that the document originated from the owner of the public key and is unchanged
- Major question—who is the owner of that public key?
  - direct trust
    - » you acquire the public key in a direct communication with the owner
    - » the model for PGP (pretty good privacy)
    - » problems of scale and responsibility
  - hierarchical or chain of trust
    - » a trusted authority, the certification authority (CA), binds the user's identity to the public key in a signed certificate
    - » X.509 model

© Hoyt L. Kesterson II, Slide 32 hoytkesterson@earthlink.net



Encrypting a message

- Sender and receiver must agree on key
- One key exchange method uses reversible asymmetric encryption

Message

Encrypt Function

Message Encrypted with Generated Key

Generate key

Symmetric Key Value

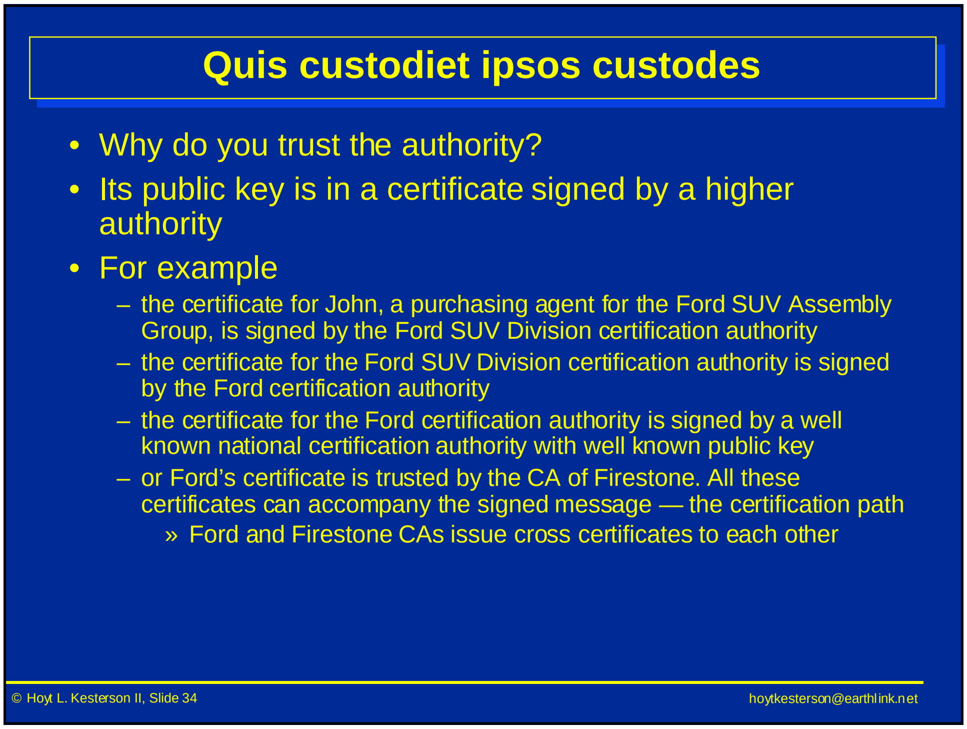
Encrypt Function

Encrypted Key

Public Key from target's certificate

- Other methods allow both users to generate the same key value, e.g. using each other's public key value
- Like for digital signature, the public key value is bound to the target in a certificate signed by a trusted authority

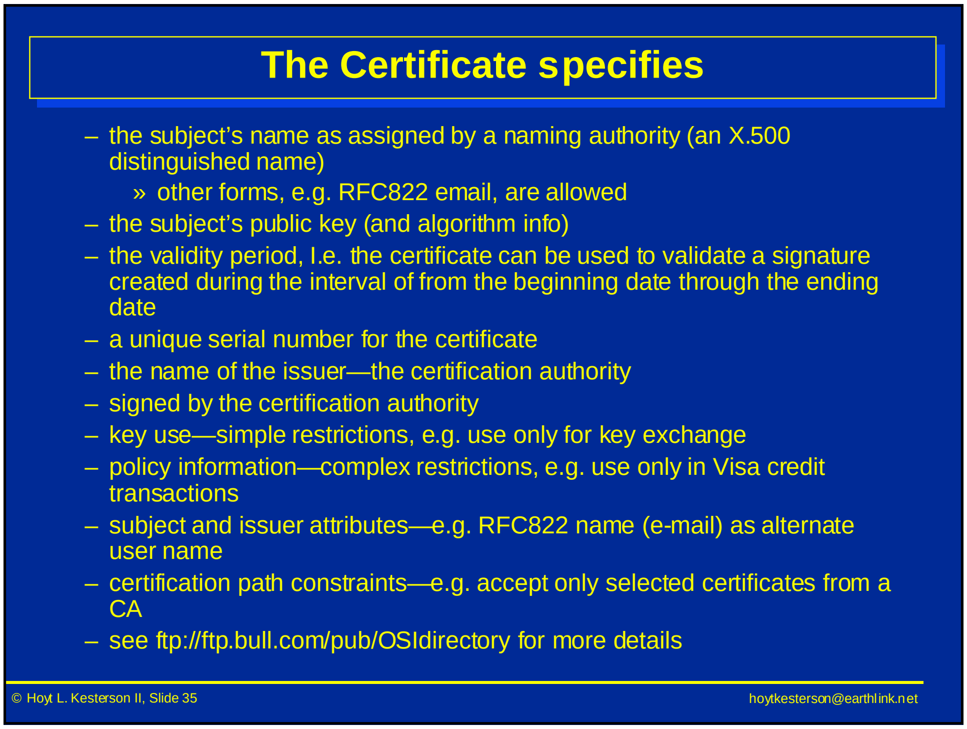
© Hoyt L. Kesterson II, Slide 33 hoytkesterson@earthlink.net



Quis custodiet ipsos custodes

- Why do you trust the authority?
- Its public key is in a certificate signed by a higher authority
- For example
  - the certificate for John, a purchasing agent for the Ford SUV Assembly Group, is signed by the Ford SUV Division certification authority
  - the certificate for the Ford SUV Division certification authority is signed by the Ford certification authority
  - the certificate for the Ford certification authority is signed by a well known national certification authority with well known public key
  - or Ford's certificate is trusted by the CA of Firestone. All these certificates can accompany the signed message — the certification path
    - » Ford and Firestone CAs issue cross certificates to each other

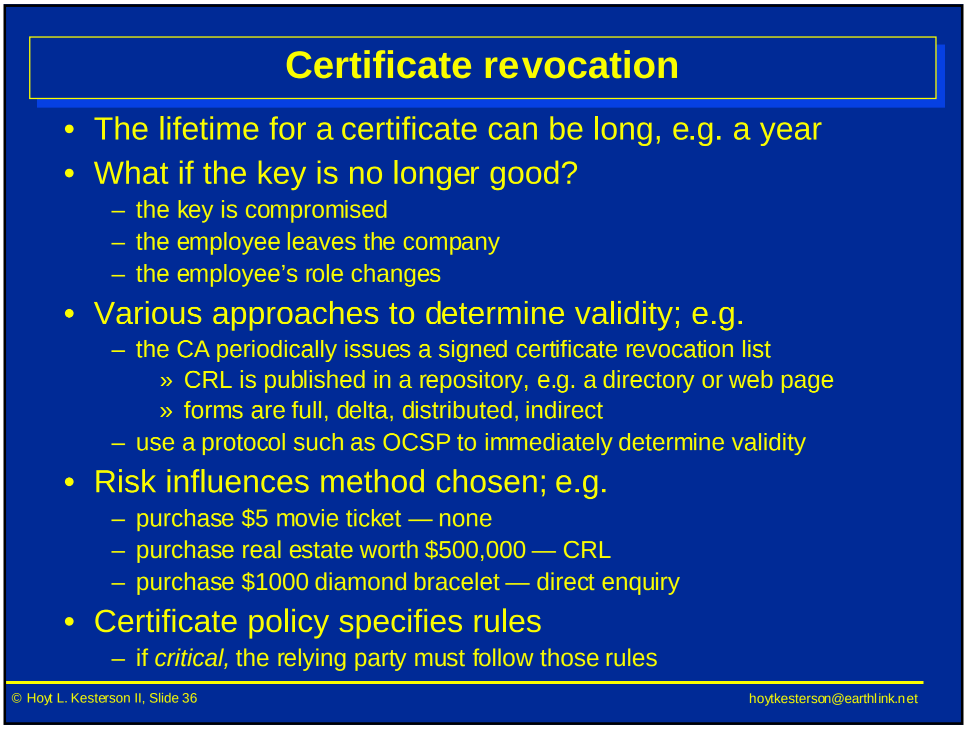
© Hoyt L. Kesterson II, Slide 34 hoytkesterson@earthlink.net



The Certificate specifies

- the subject’s name as assigned by a naming authority (an X.500 distinguished name)
  - » other forms, e.g. RFC822 email, are allowed
- the subject’s public key (and algorithm info)
- the validity period, I.e. the certificate can be used to validate a signature created during the interval of from the beginning date through the ending date
- a unique serial number for the certificate
- the name of the issuer—the certification authority
- signed by the certification authority
- key use—simple restrictions, e.g. use only for key exchange
- policy information—complex restrictions, e.g. use only in Visa credit transactions
- subject and issuer attributes—e.g. RFC822 name (e-mail) as alternate user name
- certification path constraints—e.g. accept only selected certificates from a CA
- see ftp://ftp.bull.com/pub/OSIdirectory for more details

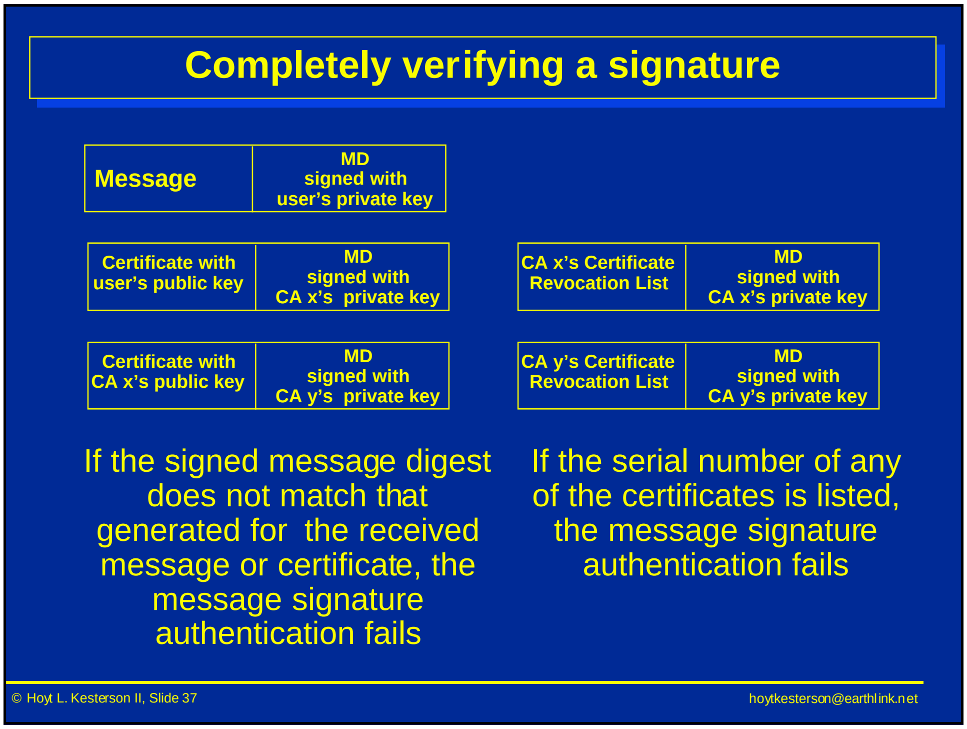
© Hoyt L. Kesterson II, Slide 35 hoytkesterson@earthlink.net



Certificate revocation

- The lifetime for a certificate can be long, e.g. a year
- What if the key is no longer good?
  - the key is compromised
  - the employee leaves the company
  - the employee’s role changes
- Various approaches to determine validity; e.g.
  - the CA periodically issues a signed certificate revocation list
    - » CRL is published in a repository, e.g. a directory or web page
    - » forms are full, delta, distributed, indirect
  - use a protocol such as OCSP to immediately determine validity
- Risk influences method chosen; e.g.
  - purchase $5 movie ticket — none
  - purchase real estate worth $500,000 — CRL
  - purchase $1000 diamond bracelet — direct enquiry
- Certificate policy specifies rules
  - if *critical,* the relying party must follow those rules

© Hoyt L. Kesterson II, Slide 36 hoytkesterson@earthlink.net



Completely verifying a signature

Message	MD signed with user's private key

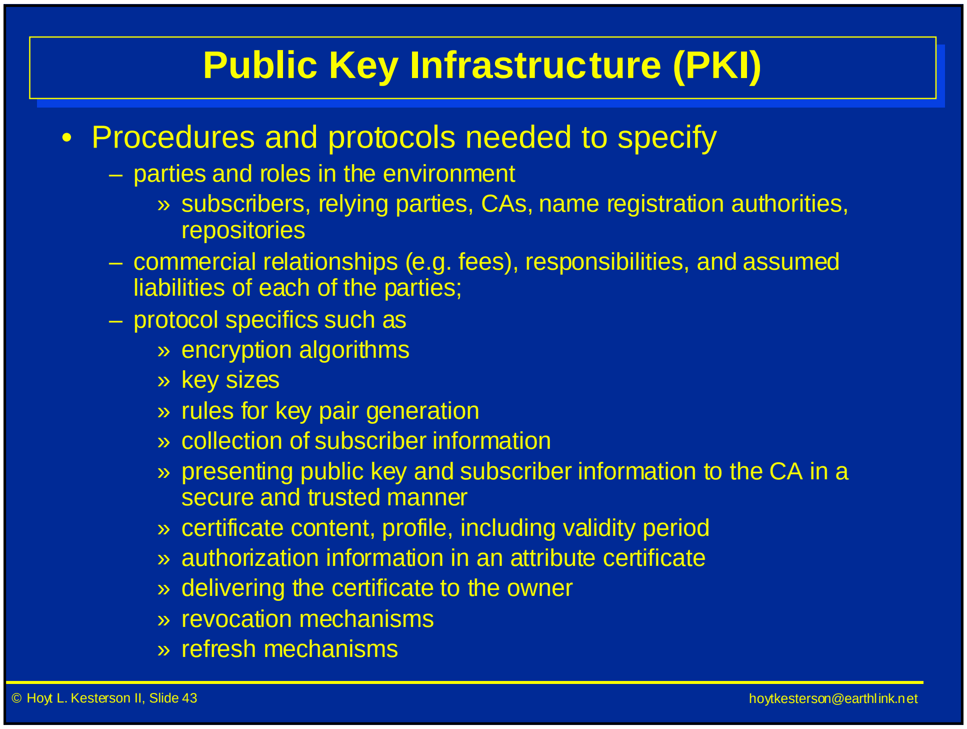
Certificate with user's public key	MD signed with CA x's private key
Certificate with CA x's public key	MD signed with CA y's private key

CA x's Certificate Revocation List	MD signed with CA x's private key
CA y's Certificate Revocation List	MD signed with CA y's private key

If the signed message digest does not match that generated for the received message or certificate, the message signature authentication fails

If the serial number of any of the certificates is listed, the message signature authentication fails

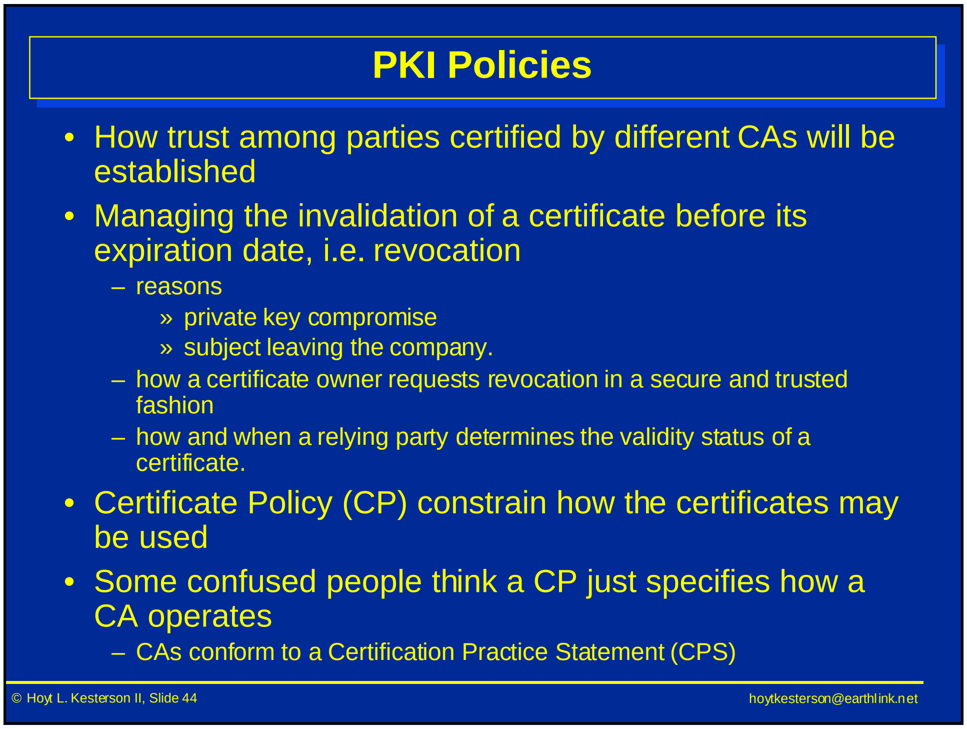
© Hoyt L. Kesterson II, Slide 37 hoytkesterson@earthlink.net



Public Key Infrastructure (PKI)

- Procedures and protocols needed to specify
  - parties and roles in the environment
    - » subscribers, relying parties, CAs, name registration authorities, repositories
  - commercial relationships (e.g. fees), responsibilities, and assumed liabilities of each of the parties;
  - protocol specifics such as
    - » encryption algorithms
    - » key sizes
    - » rules for key pair generation
    - » collection of subscriber information
    - » presenting public key and subscriber information to the CA in a secure and trusted manner
    - » certificate content, profile, including validity period
    - » authorization information in an attribute certificate
    - » delivering the certificate to the owner
    - » revocation mechanisms
    - » refresh mechanisms

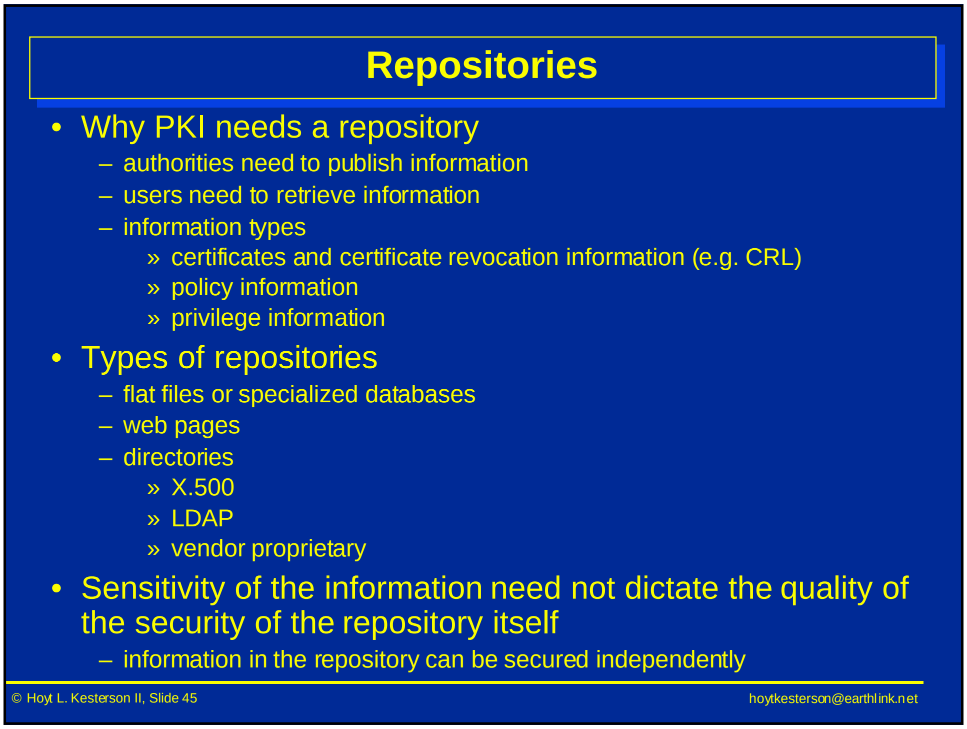
© Hoyt L. Kesterson II, Slide 43 hoytkesterson@earthlink.net



PKI Policies

- How trust among parties certified by different CAs will be established
- Managing the invalidation of a certificate before its expiration date, i.e. revocation
  - reasons
    - private key compromise
    - subject leaving the company.
  - how a certificate owner requests revocation in a secure and trusted fashion
  - how and when a relying party determines the validity status of a certificate.
- Certificate Policy (CP) constrain how the certificates may be used
- Some confused people think a CP just specifies how a CA operates
  - CAs conform to a Certification Practice Statement (CPS)

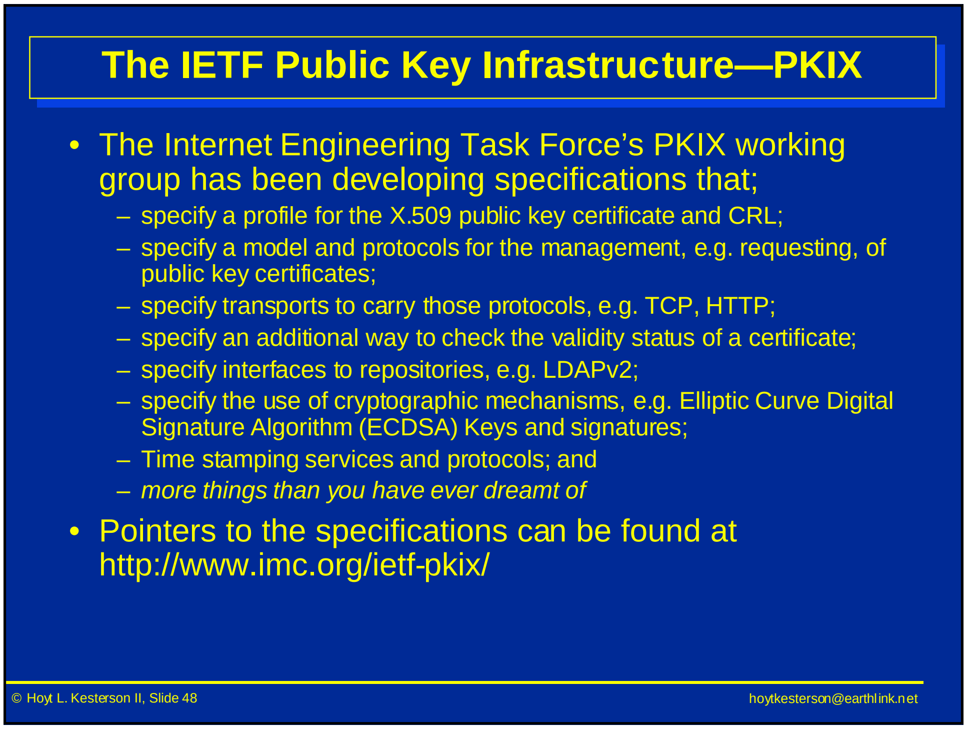
© Hoyt L. Kesterson II, Slide 44 hoytkesterson@earthlink.net



Repositories

- Why PKI needs a repository
  - authorities need to publish information
  - users need to retrieve information
  - information types
    - certificates and certificate revocation information (e.g. CRL)
    - policy information
    - privilege information
- Types of repositories
  - flat files or specialized databases
  - web pages
  - directories
    - X.500
    - LDAP
    - vendor proprietary
- Sensitivity of the information need not dictate the quality of the security of the repository itself
  - information in the repository can be secured independently

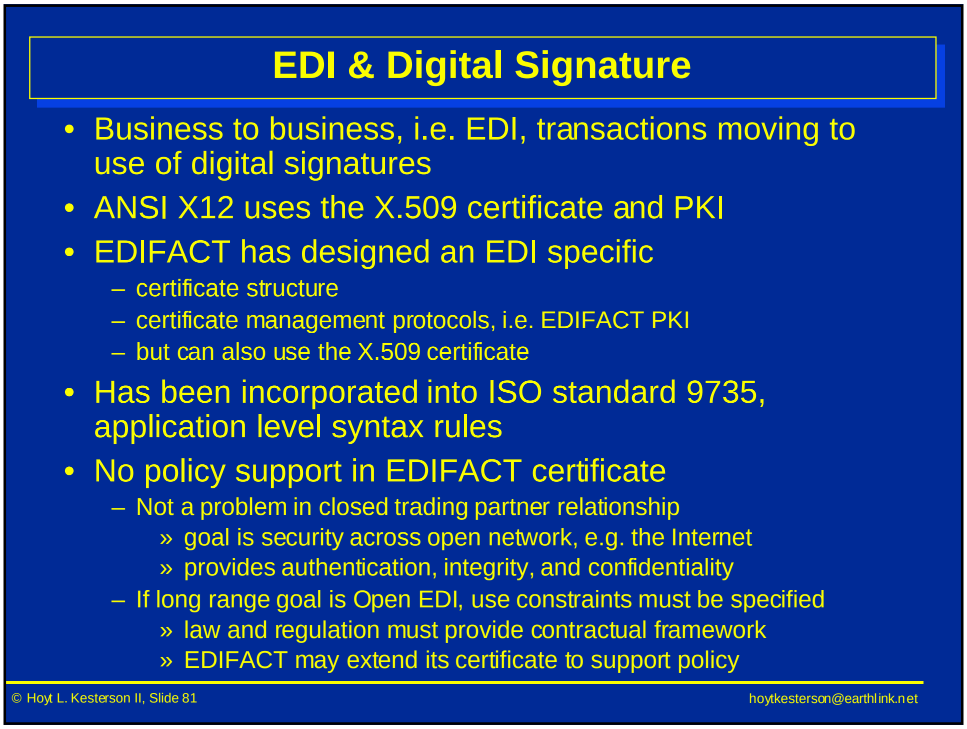
© Hoyt L. Kesterson II, Slide 45 hoytkesterson@earthlink.net



The IETF Public Key Infrastructure—PKIX

- The Internet Engineering Task Force's PKIX working group has been developing specifications that;
  - specify a profile for the X.509 public key certificate and CRL;
  - specify a model and protocols for the management, e.g. requesting, of public key certificates;
  - specify transports to carry those protocols, e.g. TCP, HTTP;
  - specify an additional way to check the validity status of a certificate;
  - specify interfaces to repositories, e.g. LDAPv2;
  - specify the use of cryptographic mechanisms, e.g. Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and signatures;
  - Time stamping services and protocols; and
  - *more things than you have ever dreamt of*
- Pointers to the specifications can be found at http://www.imc.org/ietf-pkix/

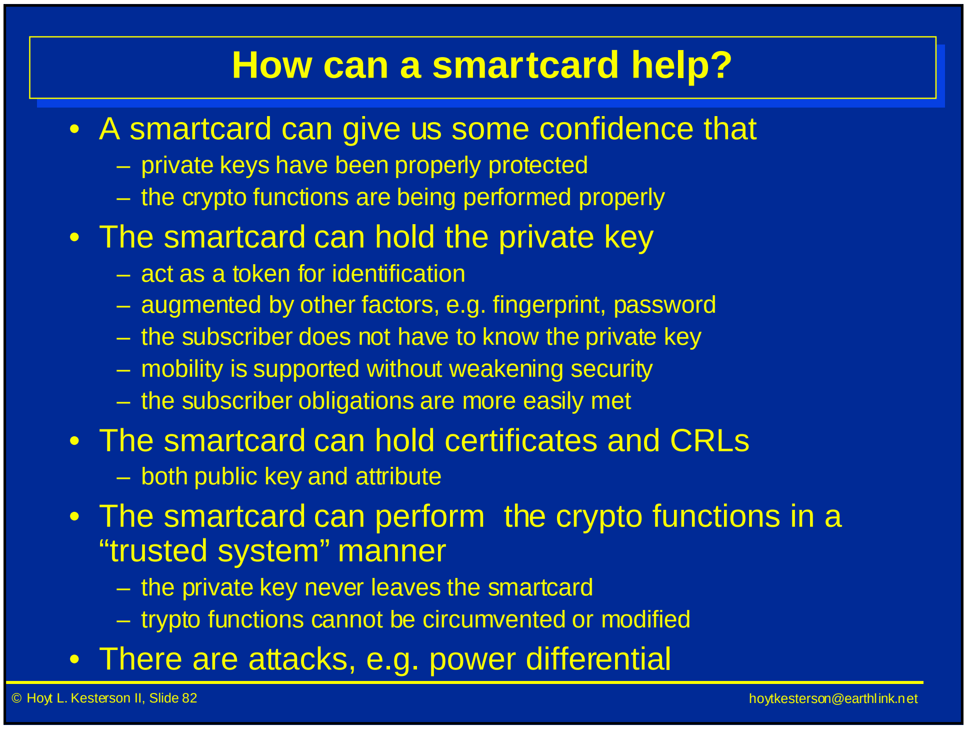
© Hoyt L. Kesterson II, Slide 48 hoytkesterson@earthlink.net



EDI & Digital Signature

- Business to business, i.e. EDI, transactions moving to use of digital signatures
- ANSI X12 uses the X.509 certificate and PKI
- EDIFACT has designed an EDI specific
  - certificate structure
  - certificate management protocols, i.e. EDIFACT PKI
  - but can also use the X.509 certificate
- Has been incorporated into ISO standard 9735, application level syntax rules
- No policy support in EDIFACT certificate
  - Not a problem in closed trading partner relationship
    - » goal is security across open network, e.g. the Internet
    - » provides authentication, integrity, and confidentiality
  - If long range goal is Open EDI, use constraints must be specified
    - » law and regulation must provide contractual framework
    - » EDIFACT may extend its certificate to support policy

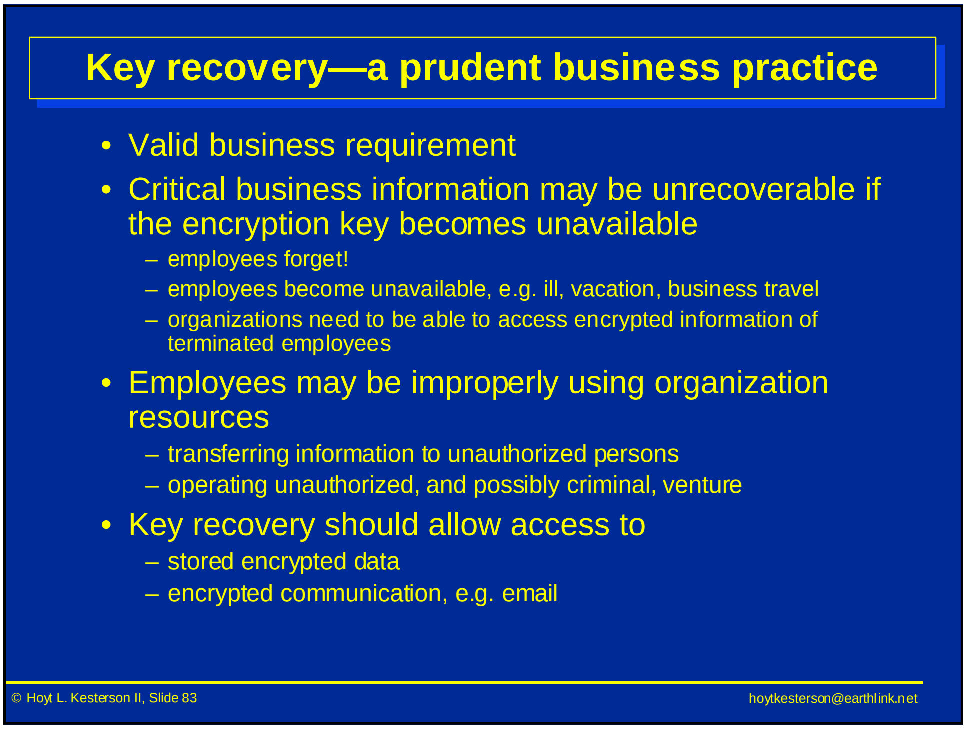
© Hoyt L. Kesterson II, Slide 81 hoytkesterson@earthlink.net



How can a smartcard help?

- A smartcard can give us some confidence that
  - – private keys have been properly protected
  - – the crypto functions are being performed properly
- The smartcard can hold the private key
  - – act as a token for identification
  - – augmented by other factors, e.g. fingerprint, password
  - – the subscriber does not have to know the private key
  - – mobility is supported without weakening security
  - – the subscriber obligations are more easily met
- The smartcard can hold certificates and CRLs
  - – both public key and attribute
- The smartcard can perform the crypto functions in a “trusted system” manner
  - – the private key never leaves the smartcard
  - – trypto functions cannot be circumvented or modified
- There are attacks, e.g. power differential

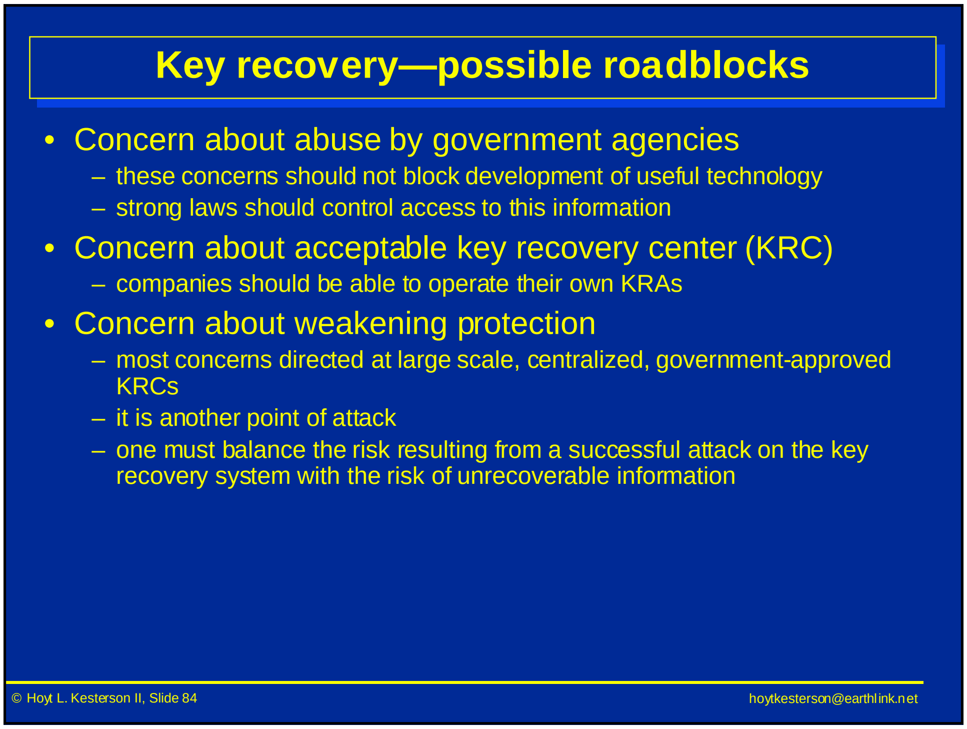
© Hoyt L. Kesterson II, Slide 82 hoytkesterson@earthlink.net



Key recovery—a prudent business practice

- Valid business requirement
- Critical business information may be unrecoverable if the encryption key becomes unavailable
  - – employees forget!
  - – employees become unavailable, e.g. ill, vacation, business travel
  - – organizations need to be able to access encrypted information of terminated employees
- Employees may be improperly using organization resources
  - – transferring information to unauthorized persons
  - – operating unauthorized, and possibly criminal, venture
- Key recovery should allow access to
  - – stored encrypted data
  - – encrypted communication, e.g. email

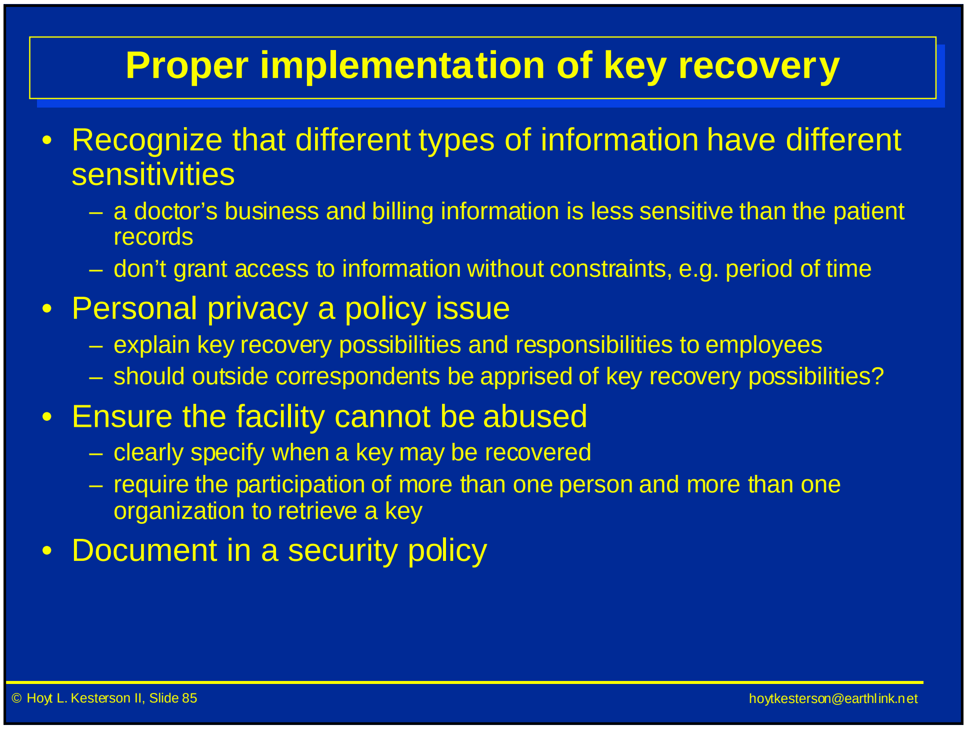
© Hoyt L. Kesterson II, Slide 83 hoytkesterson@earthlink.net



Key recovery—possible roadblocks

- Concern about abuse by government agencies
  - these concerns should not block development of useful technology
  - strong laws should control access to this information
- Concern about acceptable key recovery center (KRC)
  - companies should be able to operate their own KRAs
- Concern about weakening protection
  - most concerns directed at large scale, centralized, government-approved KRCs
  - it is another point of attack
  - one must balance the risk resulting from a successful attack on the key recovery system with the risk of unrecoverable information

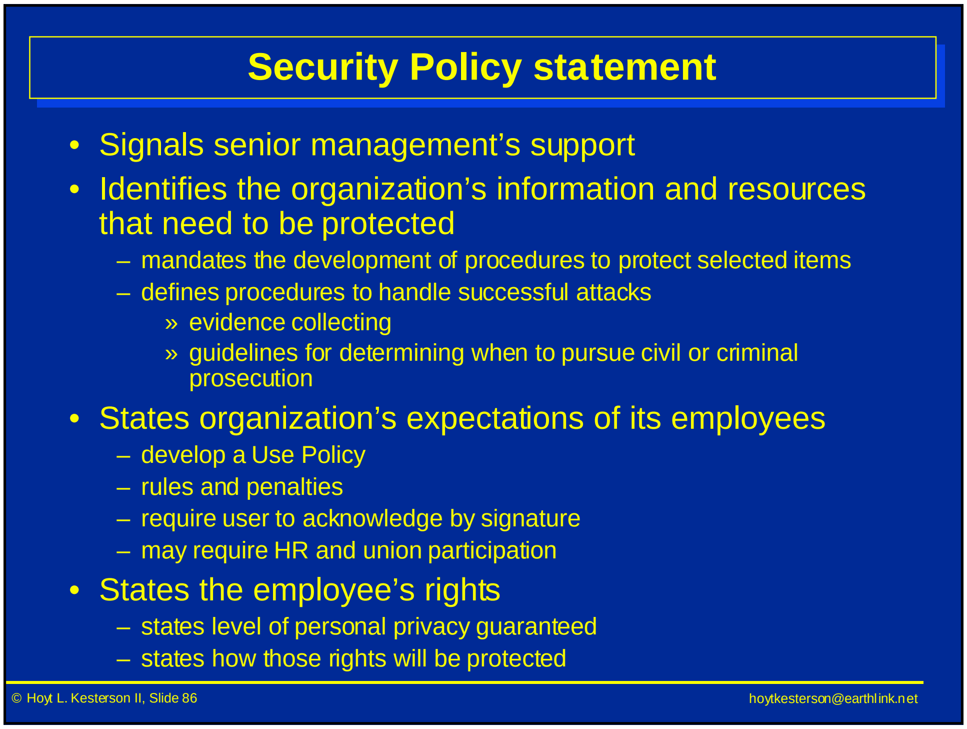
© Hoyt L. Kesterson II, Slide 84 hoytkesterson@earthlink.net



Proper implementation of key recovery

- Recognize that different types of information have different sensitivities
  - a doctor’s business and billing information is less sensitive than the patient records
  - don’t grant access to information without constraints, e.g. period of time
- Personal privacy a policy issue
  - explain key recovery possibilities and responsibilities to employees
  - should outside correspondents be apprised of key recovery possibilities?
- Ensure the facility cannot be abused
  - clearly specify when a key may be recovered
  - require the participation of more than one person and more than one organization to retrieve a key
- Document in a security policy

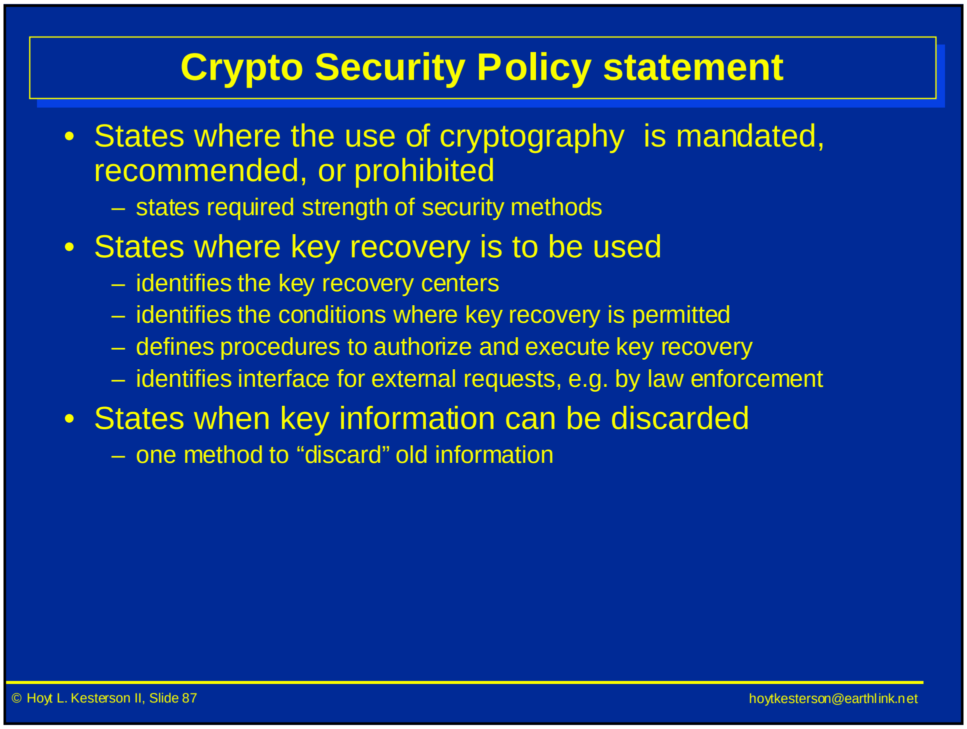
© Hoyt L. Kesterson II, Slide 85 hoytkesterson@earthlink.net



Security Policy statement

- Signals senior management’s support
- Identifies the organization’s information and resources that need to be protected
  - – mandates the development of procedures to protect selected items
  - – defines procedures to handle successful attacks
    - » evidence collecting
    - » guidelines for determining when to pursue civil or criminal prosecution
- States organization’s expectations of its employees
  - – develop a Use Policy
  - – rules and penalties
  - – require user to acknowledge by signature
  - – may require HR and union participation
- States the employee’s rights
  - – states level of personal privacy guaranteed
  - – states how those rights will be protected

© Hoyt L. Kesterson II, Slide 86 hoytkesterson@earthlink.net

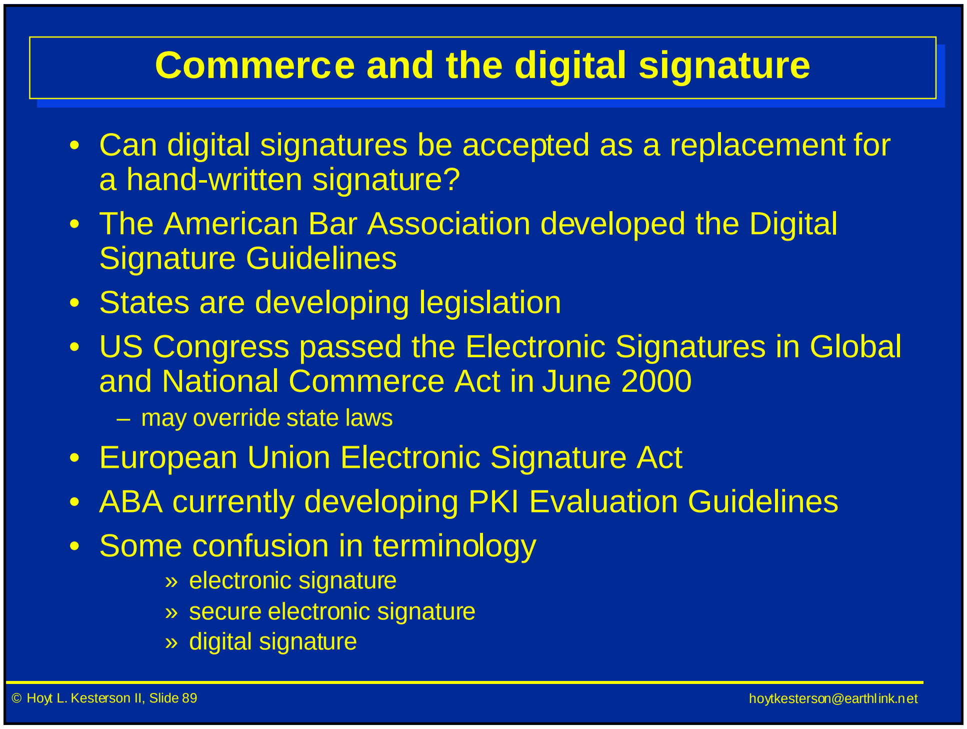


Crypto Security Policy statement

- States where the use of cryptography is mandated, recommended, or prohibited
  - – states required strength of security methods
- States where key recovery is to be used
  - – identifies the key recovery centers
  - – identifies the conditions where key recovery is permitted
  - – defines procedures to authorize and execute key recovery
  - – identifies interface for external requests, e.g. by law enforcement
- States when key information can be discarded
  - – one method to “discard” old information

© Hoyt L. Kesterson II, Slide 87 hoytkesterson@earthlink.net

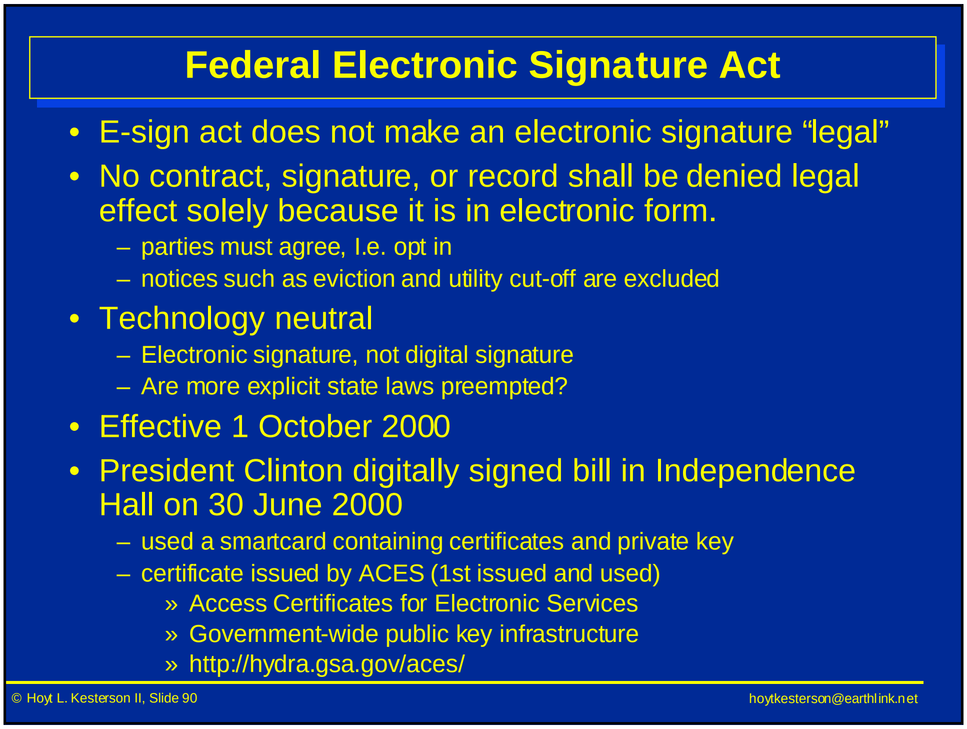
I am
Not a
Lawyer



Commerce and the digital signature

- Can digital signatures be accepted as a replacement for a hand-written signature?
- The American Bar Association developed the Digital Signature Guidelines
- States are developing legislation
- US Congress passed the Electronic Signatures in Global and National Commerce Act in June 2000
  - may override state laws
- European Union Electronic Signature Act
- ABA currently developing PKI Evaluation Guidelines
- Some confusion in terminology
  - » electronic signature
  - » secure electronic signature
  - » digital signature

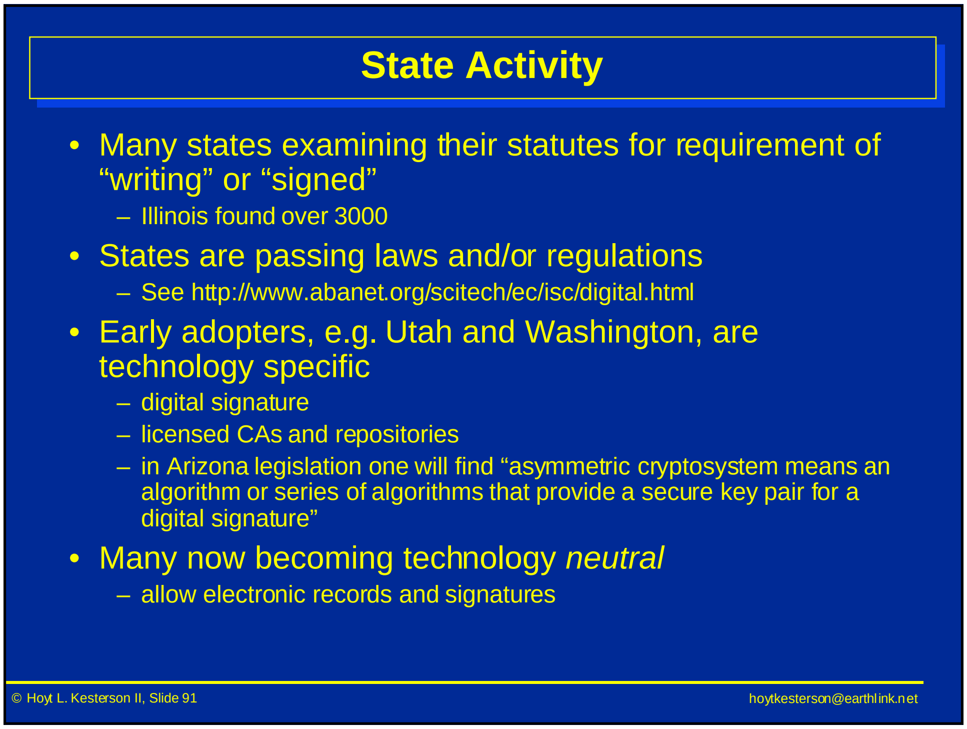
© Hoyt L. Kesterson II, Slide 89 hoytkesterson@earthlink.net



Federal Electronic Signature Act

- E-sign act does not make an electronic signature “legal”
- No contract, signature, or record shall be denied legal effect solely because it is in electronic form.
  - parties must agree, I.e. opt in
  - notices such as eviction and utility cut-off are excluded
- Technology neutral
  - Electronic signature, not digital signature
  - Are more explicit state laws preempted?
- Effective 1 October 2000
- President Clinton digitally signed bill in Independence Hall on 30 June 2000
  - used a smartcard containing certificates and private key
  - certificate issued by ACES (1st issued and used)
    - » Access Certificates for Electronic Services
    - » Government-wide public key infrastructure
    - » http://hydra.gsa.gov/aces/

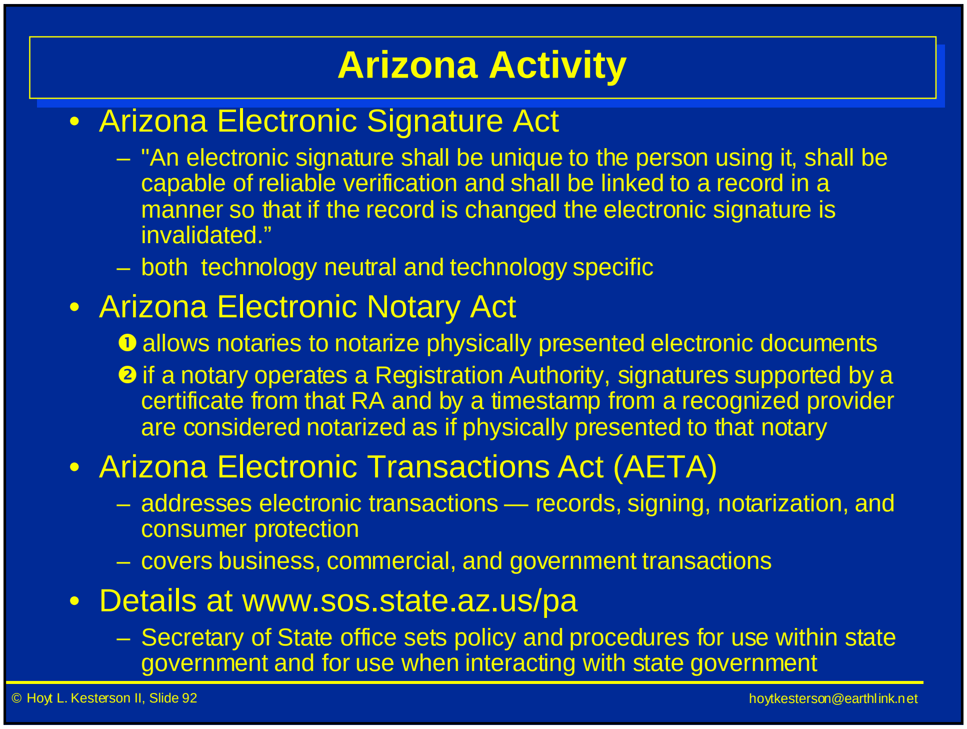
© Hoyt L. Kesterson II, Slide 90 hoytkesterson@earthlink.net



State Activity

- Many states examining their statutes for requirement of “writing” or “signed”
  - Illinois found over 3000
- States are passing laws and/or regulations
  - See http://www.abanet.org/scitech/ec/isc/digital.html
- Early adopters, e.g. Utah and Washington, are technology specific
  - digital signature
  - licensed CAs and repositories
  - in Arizona legislation one will find “asymmetric cryptosystem means an algorithm or series of algorithms that provide a secure key pair for a digital signature”
- Many now becoming technology *neutral*
  - allow electronic records and signatures

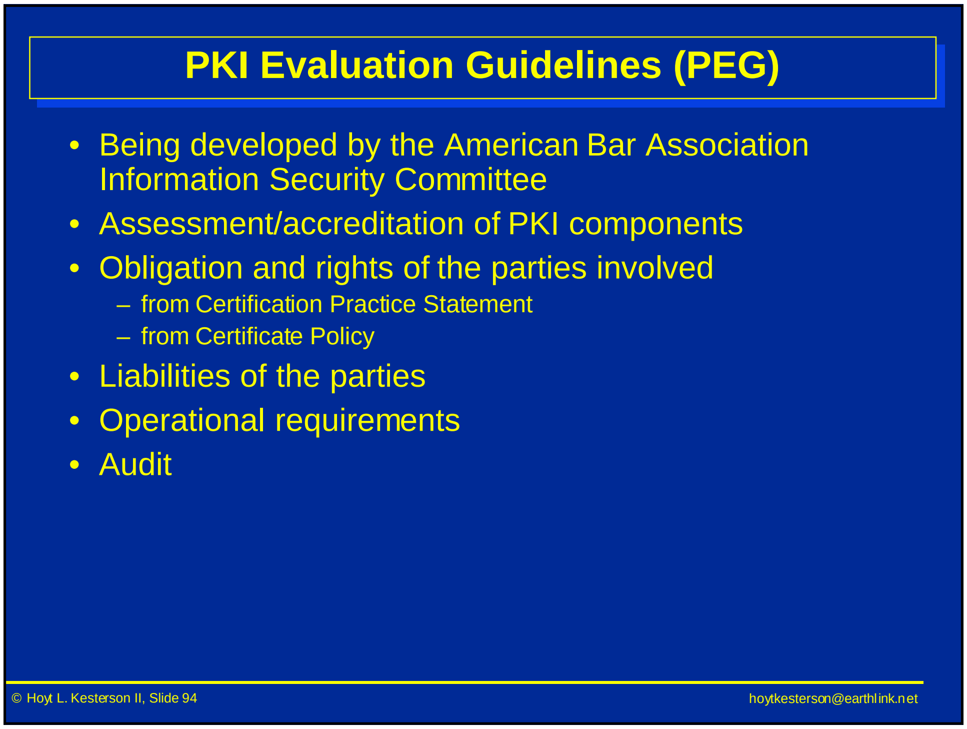
© Hoyt L. Kesterson II, Slide 91 hoytkesterson@earthlink.net



Arizona Activity

- Arizona Electronic Signature Act
  - "An electronic signature shall be unique to the person using it, shall be capable of reliable verification and shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated."
  - both technology neutral and technology specific
- Arizona Electronic Notary Act
  - ❶ allows notaries to notarize physically presented electronic documents
  - ❷ if a notary operates a Registration Authority, signatures supported by a certificate from that RA and by a timestamp from a recognized provider are considered notarized as if physically presented to that notary
- Arizona Electronic Transactions Act (AETA)
  - addresses electronic transactions — records, signing, notarization, and consumer protection
  - covers business, commercial, and government transactions
- Details at www.sos.state.az.us/pa
  - Secretary of State office sets policy and procedures for use within state government and for use when interacting with state government

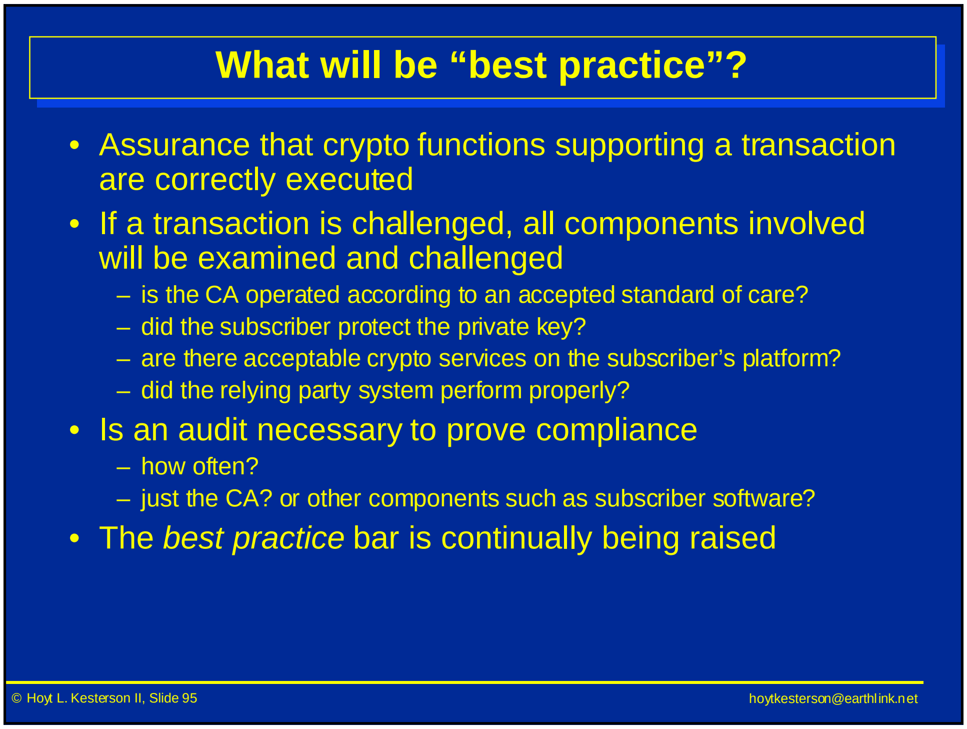
© Hoyt L. Kesterson II, Slide 92 hoytkesterson@earthlink.net



PKI Evaluation Guidelines (PEG)

- Being developed by the American Bar Association Information Security Committee
- Assessment/accreditation of PKI components
- Obligation and rights of the parties involved
  - from Certification Practice Statement
  - from Certificate Policy
- Liabilities of the parties
- Operational requirements
- Audit

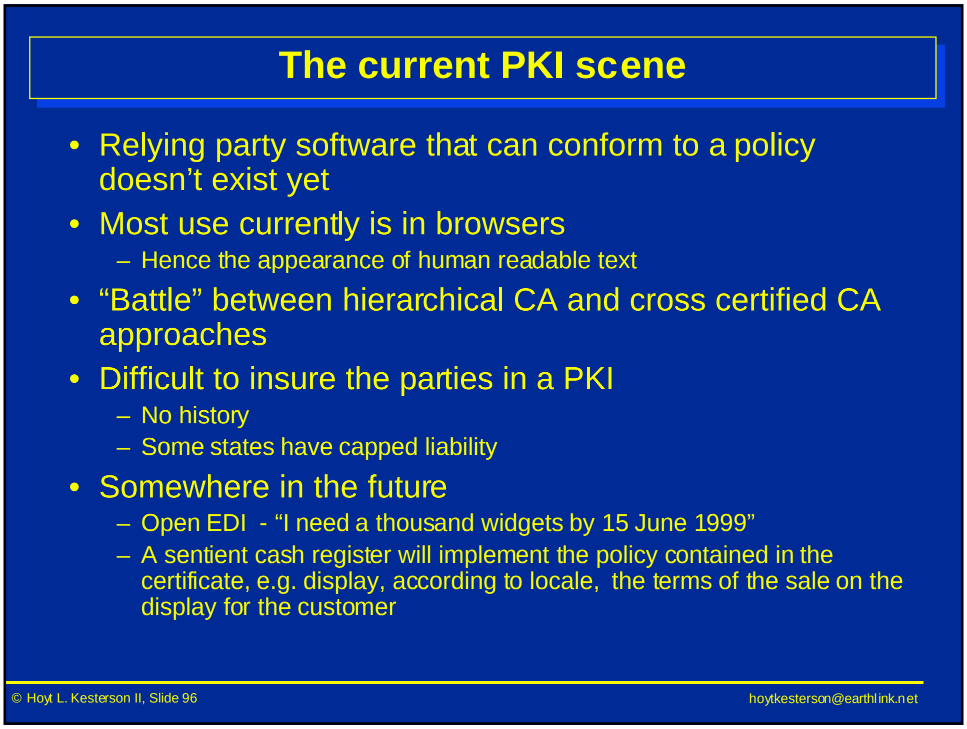
© Hoyt L. Kesterson II, Slide 94 hoytkesterson@earthlink.net



What will be “best practice”?

- Assurance that crypto functions supporting a transaction are correctly executed
- If a transaction is challenged, all components involved will be examined and challenged
  - is the CA operated according to an accepted standard of care?
  - did the subscriber protect the private key?
  - are there acceptable crypto services on the subscriber’s platform?
  - did the relying party system perform properly?
- Is an audit necessary to prove compliance
  - how often?
  - just the CA? or other components such as subscriber software?
- The *best practice* bar is continually being raised

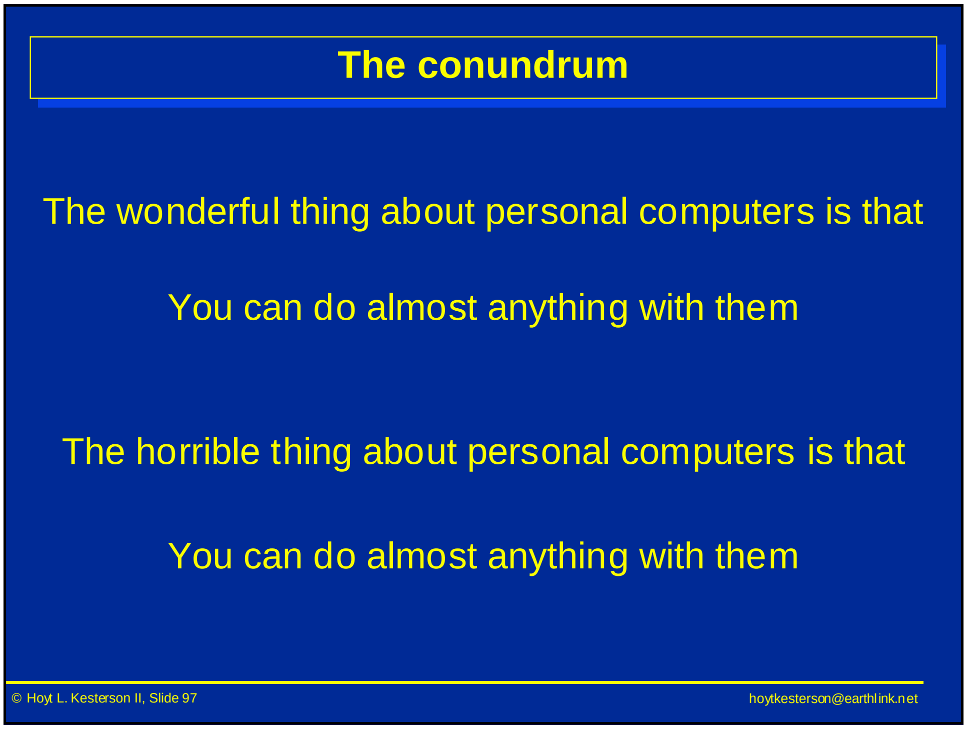
© Hoyt L. Kesterson II, Slide 95 hoytkesterson@earthlink.net



The current PKI scene

- Relying party software that can conform to a policy doesn’t exist yet
- Most use currently is in browsers
  - Hence the appearance of human readable text
- “Battle” between hierarchical CA and cross certified CA approaches
- Difficult to insure the parties in a PKI
  - No history
  - Some states have capped liability
- Somewhere in the future
  - Open EDI - “I need a thousand widgets by 15 June 1999”
  - A sentient cash register will implement the policy contained in the certificate, e.g. display, according to locale, the terms of the sale on the display for the customer

© Hoyt L. Kesterson II, Slide 96 hoytkesterson@earthlink.net



The conundrum

The wonderful thing about personal computers is that

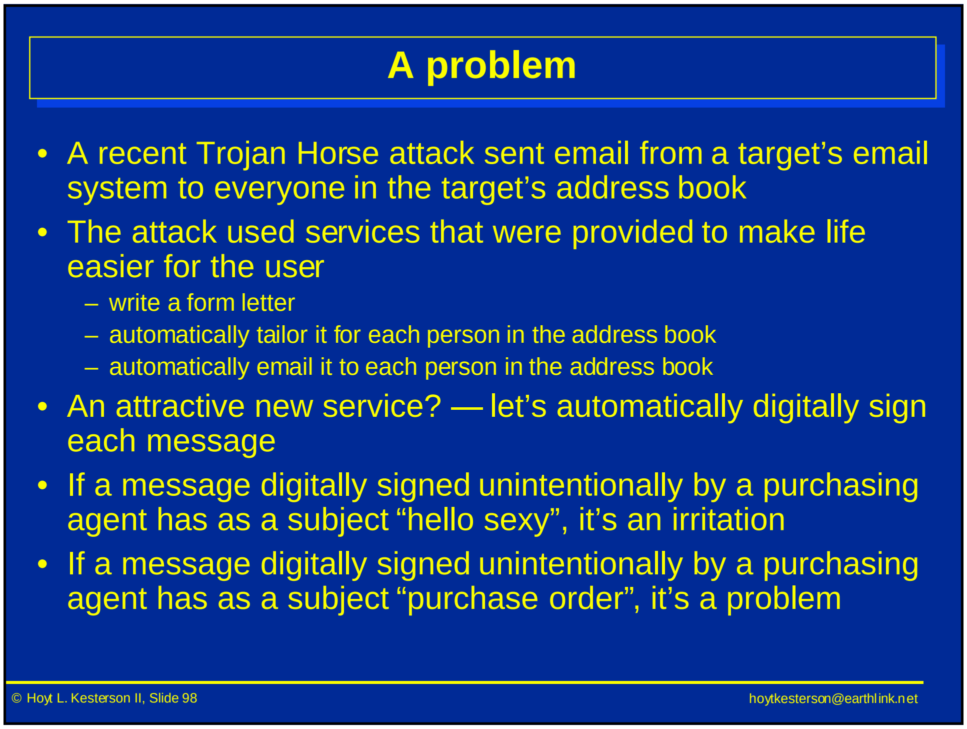
You can do almost anything with them

The horrible thing about personal computers is that

You can do almost anything with them

© Hoyt L. Kesterson II, Slide 97

hoytkesterson@earthlink.net

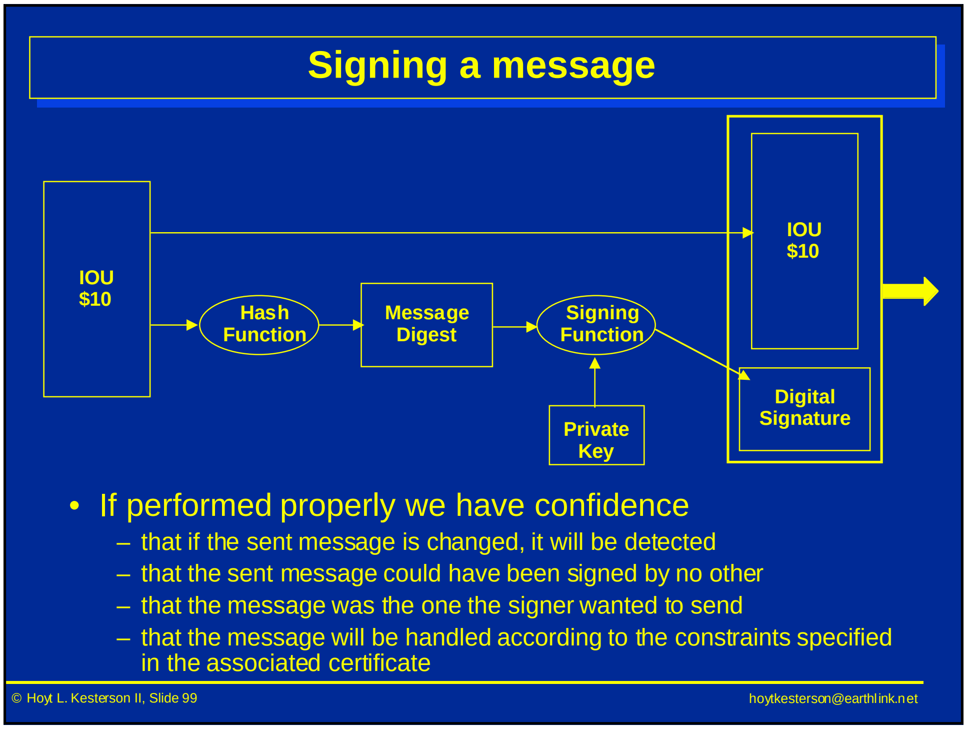


A problem

- A recent Trojan Horse attack sent email from a target’s email system to everyone in the target’s address book
- The attack used services that were provided to make life easier for the user
  - write a form letter
  - automatically tailor it for each person in the address book
  - automatically email it to each person in the address book
- An attractive new service? — let’s automatically digitally sign each message
- If a message digitally signed unintentionally by a purchasing agent has as a subject “hello sexy”, it’s an irritation
- If a message digitally signed unintentionally by a purchasing agent has as a subject “purchase order”, it’s a problem

© Hoyt L. Kesterson II, Slide 98

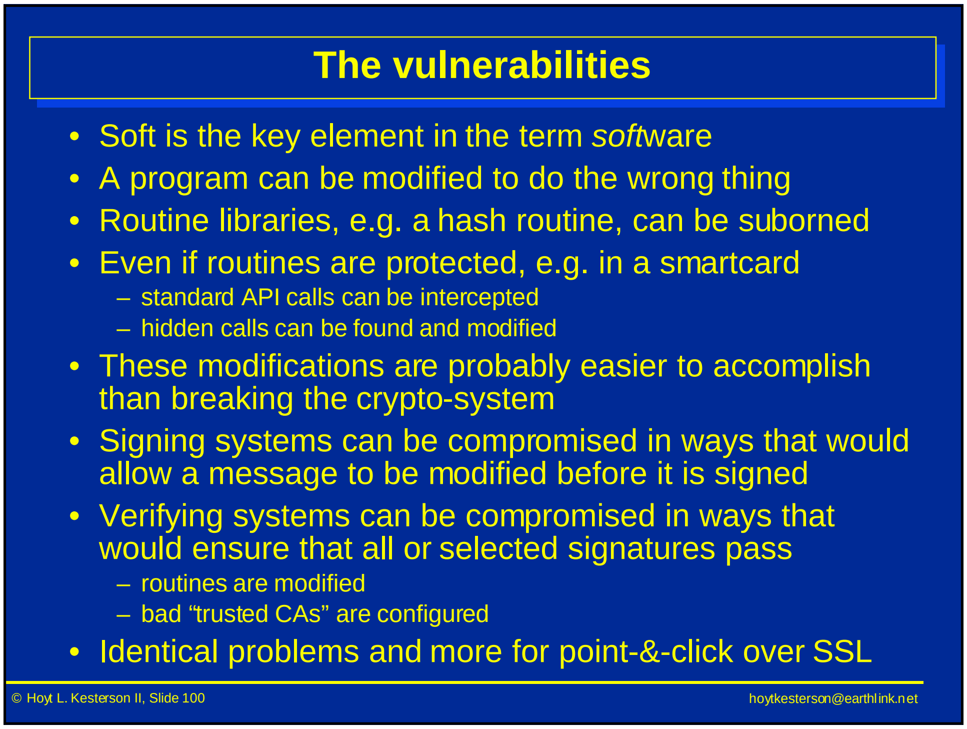
hoytkesterson@earthlink.net



Signing a message

- If performed properly we have confidence
  - that if the sent message is changed, it will be detected
  - that the sent message could have been signed by no other
  - that the message was the one the signer wanted to send
  - that the message will be handled according to the constraints specified in the associated certificate

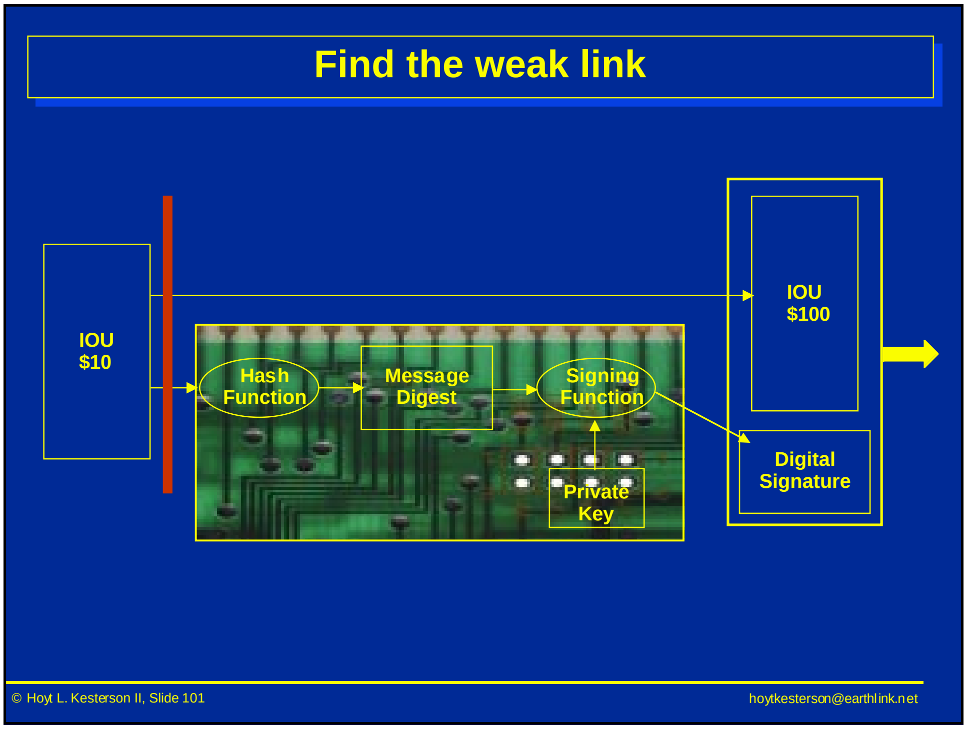
© Hoyt L. Kesterson II, Slide 99 hoytkesterson@earthlink.net



The vulnerabilities

- Soft is the key element in the term *soft*ware
- A program can be modified to do the wrong thing
- Routine libraries, e.g. a hash routine, can be suborned
- Even if routines are protected, e.g. in a smartcard
  - standard API calls can be intercepted
  - hidden calls can be found and modified
- These modifications are probably easier to accomplish than breaking the crypto-system
- Signing systems can be compromised in ways that would allow a message to be modified before it is signed
- Verifying systems can be compromised in ways that would ensure that all or selected signatures pass
  - routines are modified
  - bad “trusted CAs” are configured
- Identical problems and more for point-&-click over SSL

© Hoyt L. Kesterson II, Slide 100 hoytkesterson@earthlink.net



Find the weak link

IOU
$10

Hash
Function

Message
Digest

Signing
Function

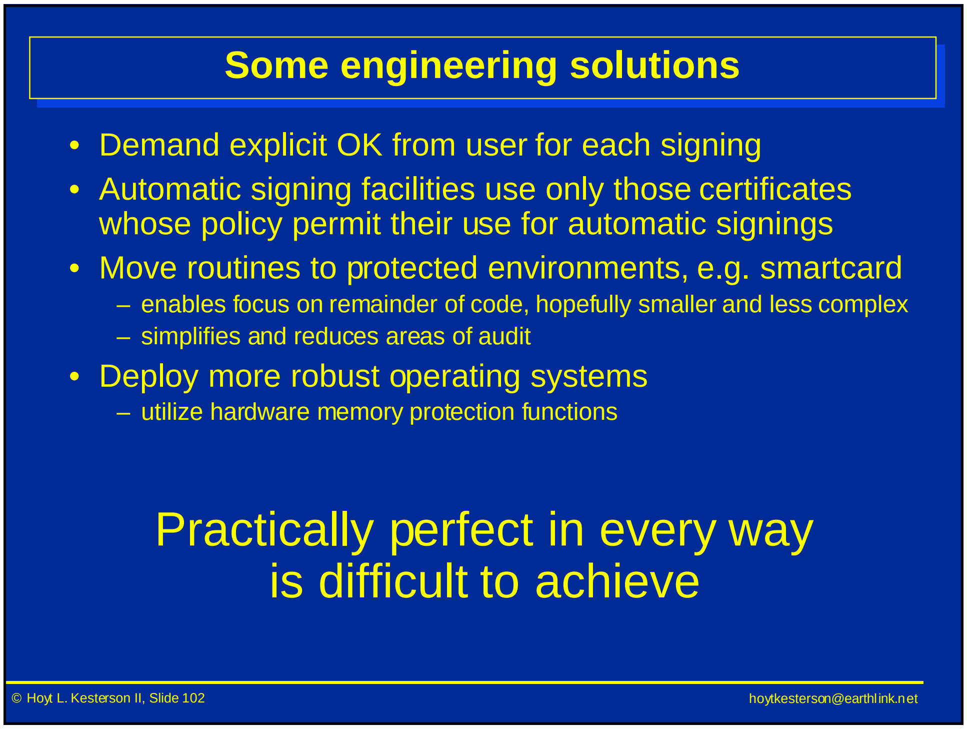
Private
Key

IOU
$100

Digital
Signature

© Hoyt L. Kesterson II, Slide 101

hoytkesterson@earthlink.net



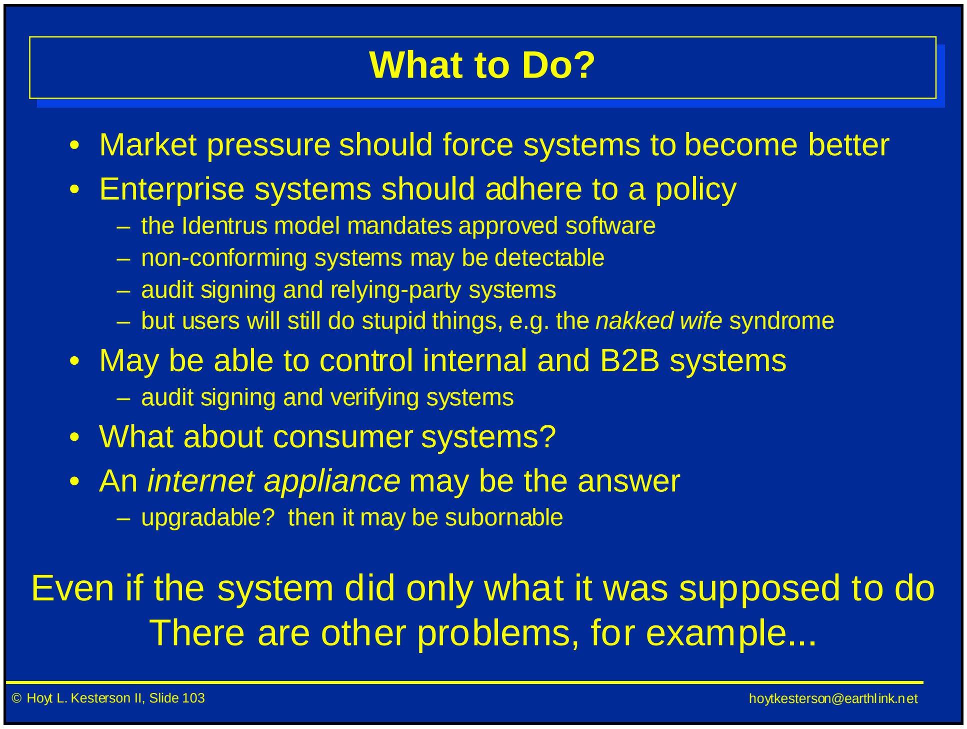
Some engineering solutions

- Demand explicit OK from user for each signing
- Automatic signing facilities use only those certificates whose policy permit their use for automatic signings
- Move routines to protected environments, e.g. smartcard
  - enables focus on remainder of code, hopefully smaller and less complex
  - simplifies and reduces areas of audit
- Deploy more robust operating systems
  - utilize hardware memory protection functions

Practically perfect in every way
is difficult to achieve

© Hoyt L. Kesterson II, Slide 102

hoytkesterson@earthlink.net



What to Do?

- Market pressure should force systems to become better
- Enterprise systems should adhere to a policy
  - the Identrus model mandates approved software
  - non-conforming systems may be detectable
  - audit signing and relying-party systems
  - but users will still do stupid things, e.g. the *nakked wife* syndrome
- May be able to control internal and B2B systems
  - audit signing and verifying systems
- What about consumer systems?
- An *internet appliance* may be the answer
  - upgradable? then it may be subornable

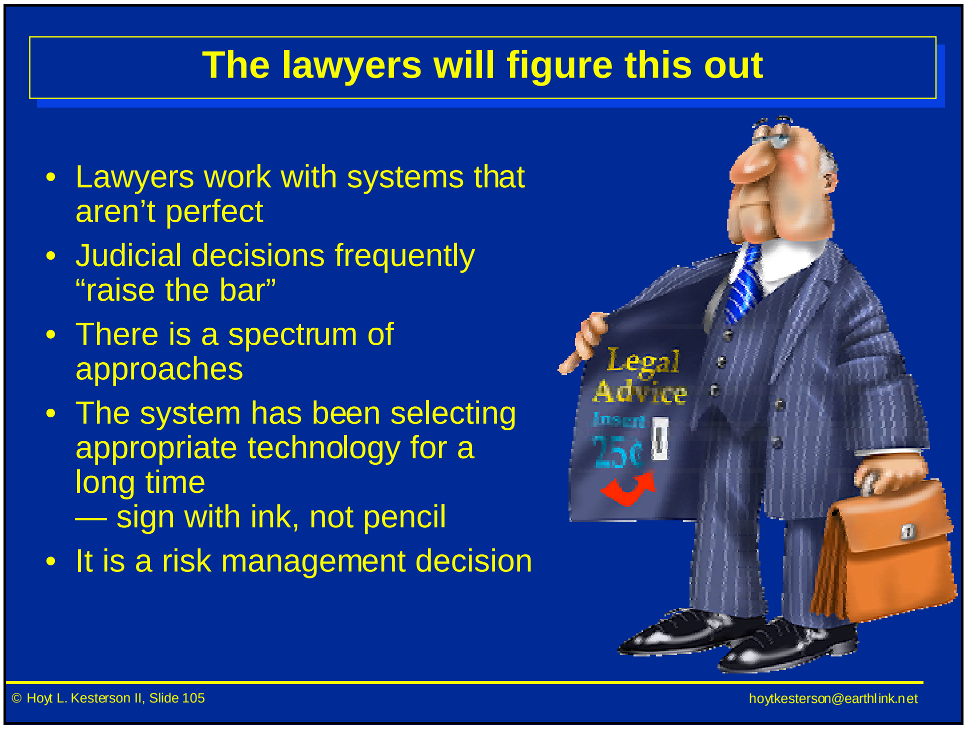
Even if the system did only what it was supposed to do
There are other problems, for example...

© Hoyt L. Kesterson II, Slide 103 hoytkesterson@earthlink.net

Was the signer forced in any way?

A technical solution to determine state of mind seems far away

© Hoyt L. Kesterson II, Slide 104 hoytkesterson@earthlink.net

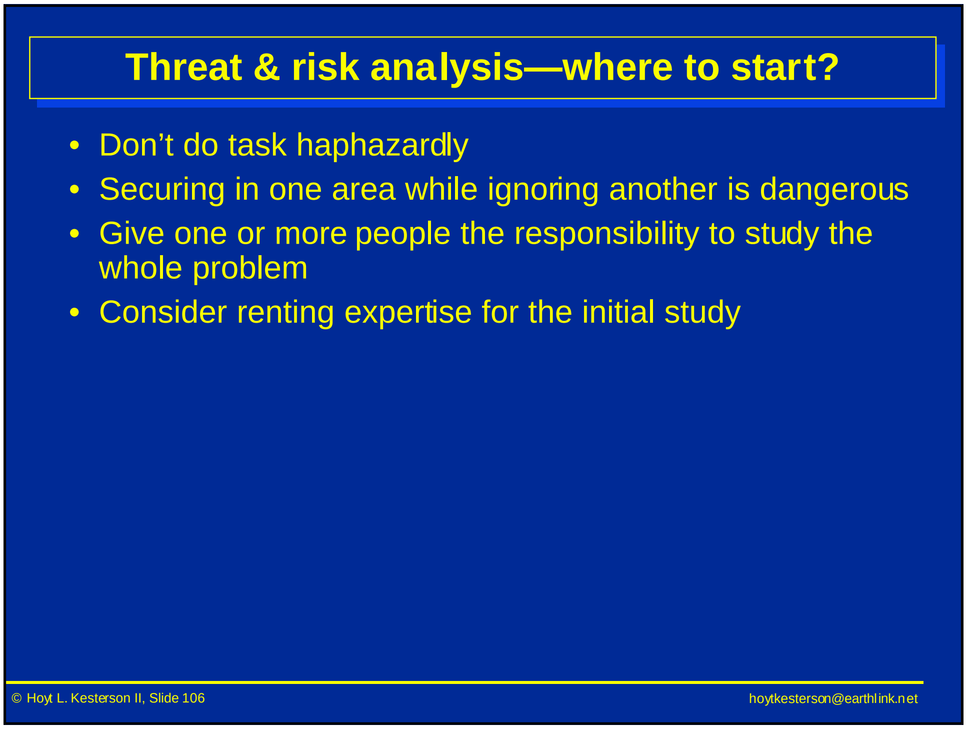


The lawyers will figure this out

- Lawyers work with systems that aren’t perfect
- Judicial decisions frequently “raise the bar”
- There is a spectrum of approaches
- The system has been selecting appropriate technology for a long time
  — sign with ink, not pencil
- It is a risk management decision

Legal
Advice
Insert
25¢

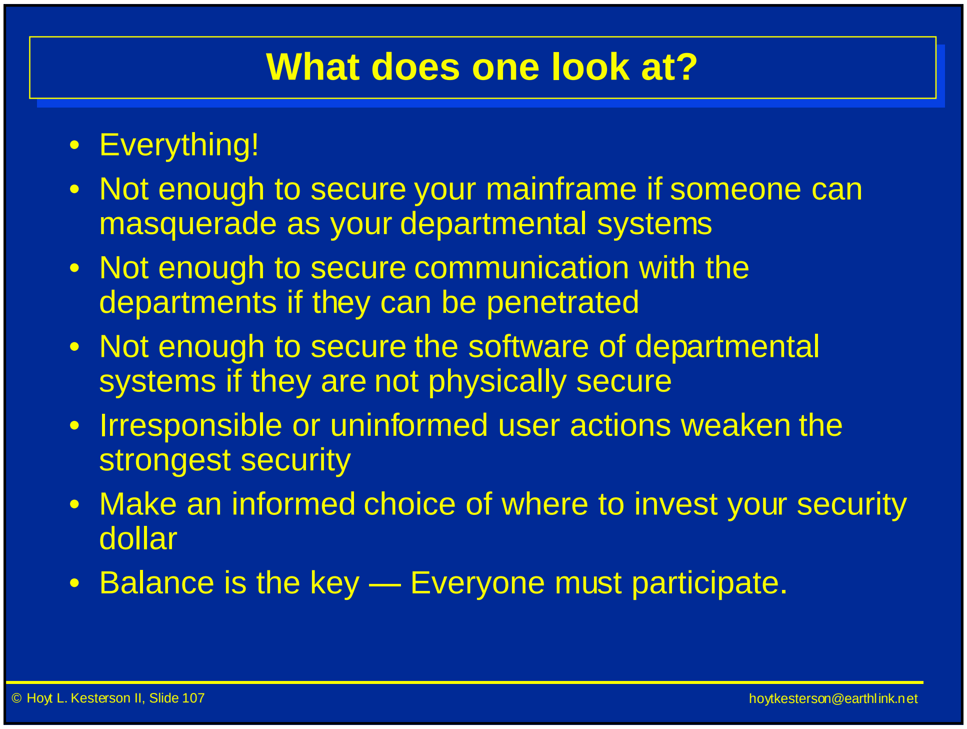
© Hoyt L. Kesterson II, Slide 105 hoytkesterson@earthlink.net



Threat & risk analysis—where to start?

- Don’t do task haphazardly
- Securing in one area while ignoring another is dangerous
- Give one or more people the responsibility to study the whole problem
- Consider renting expertise for the initial study

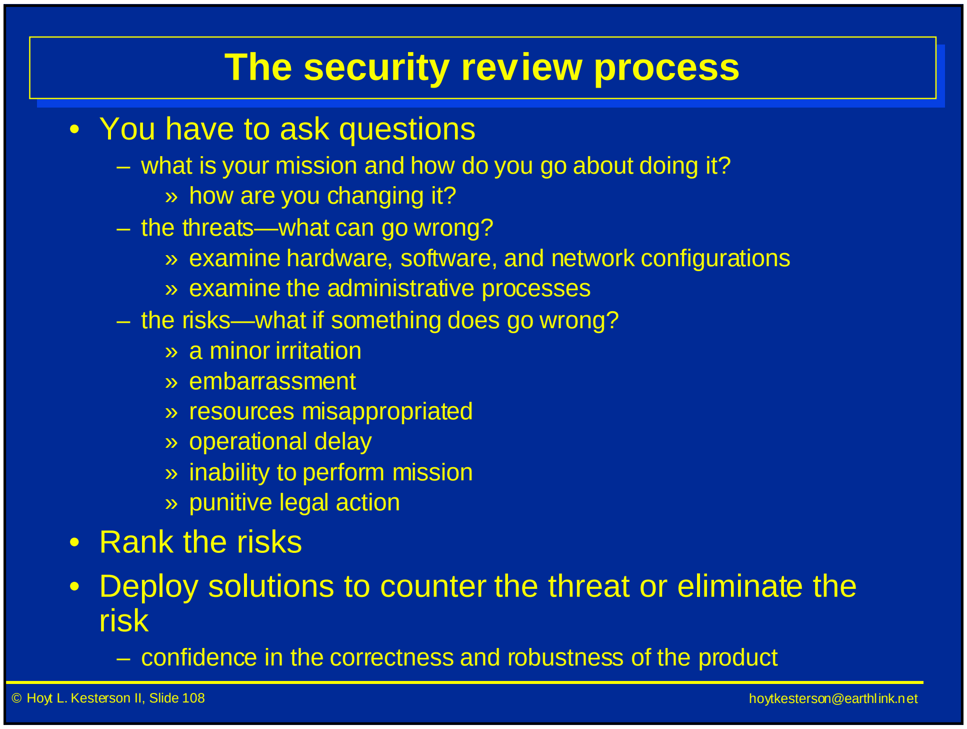
© Hoyt L. Kesterson II, Slide 106 hoytkesterson@earthlink.net



What does one look at?

- Everything!
- Not enough to secure your mainframe if someone can masquerade as your departmental systems
- Not enough to secure communication with the departments if they can be penetrated
- Not enough to secure the software of departmental systems if they are not physically secure
- Irresponsible or uninformed user actions weaken the strongest security
- Make an informed choice of where to invest your security dollar
- Balance is the key — Everyone must participate.

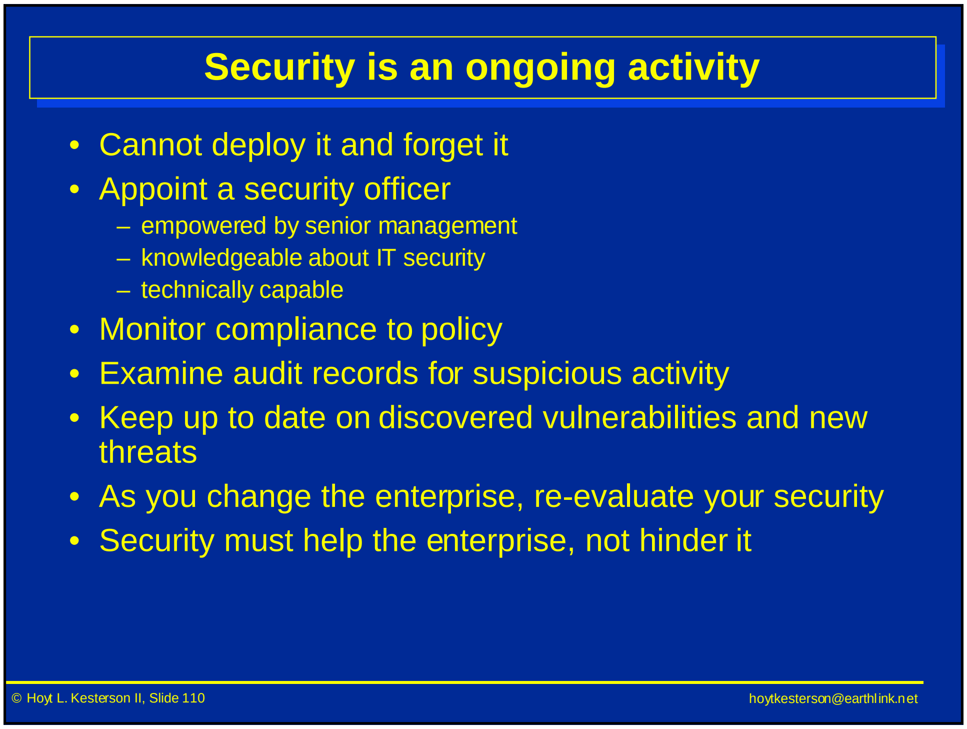
© Hoyt L. Kesterson II, Slide 107 hoytkesterson@earthlink.net



The security review process

- You have to ask questions
  - what is your mission and how do you go about doing it?
    - » how are you changing it?
  - the threats—what can go wrong?
    - » examine hardware, software, and network configurations
    - » examine the administrative processes
  - the risks—what if something does go wrong?
    - » a minor irritation
    - » embarrassment
    - » resources misappropriated
    - » operational delay
    - » inability to perform mission
    - » punitive legal action
- Rank the risks
- Deploy solutions to counter the threat or eliminate the risk
  - confidence in the correctness and robustness of the product

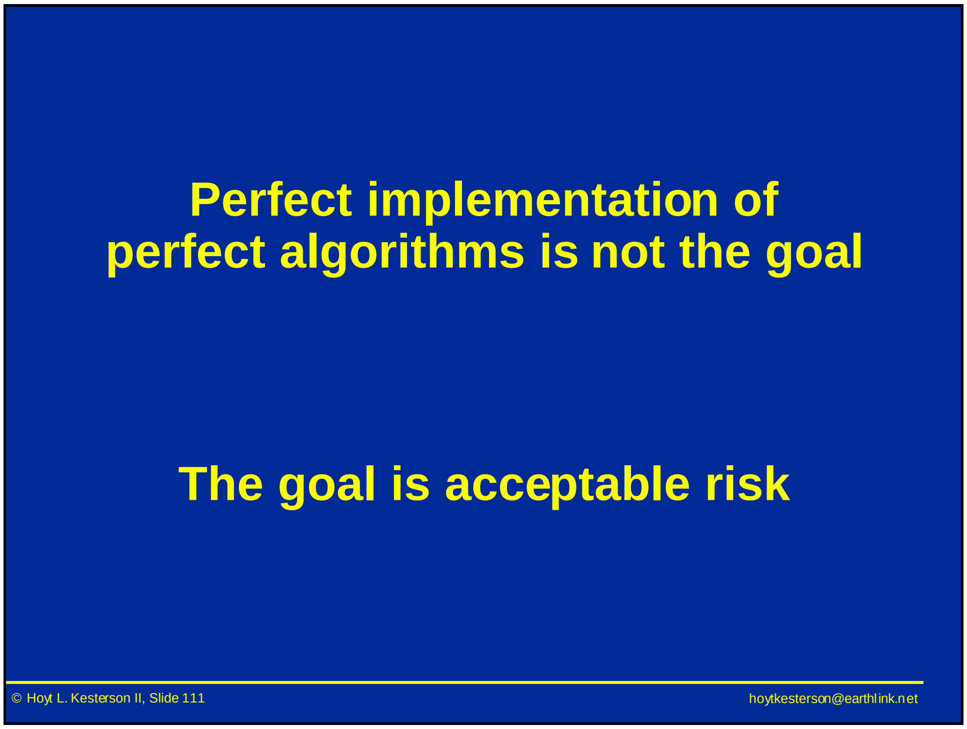
© Hoyt L. Kesterson II, Slide 108 hoytkesterson@earthlink.net



Security is an ongoing activity

- Cannot deploy it and forget it
- Appoint a security officer
  - empowered by senior management
  - knowledgeable about IT security
  - technically capable
- Monitor compliance to policy
- Examine audit records for suspicious activity
- Keep up to date on discovered vulnerabilities and new threats
- As you change the enterprise, re-evaluate your security
- Security must help the enterprise, not hinder it

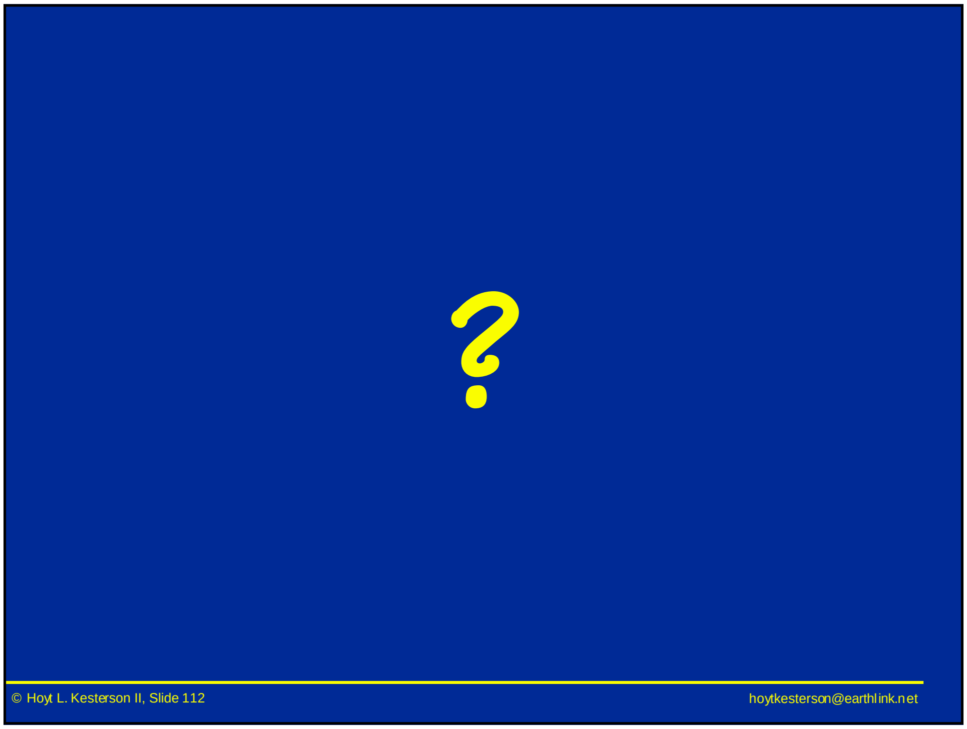
© Hoyt L. Kesterson II, Slide 110 hoytkesterson@earthlink.net



Perfect implementation of perfect algorithms is not the goal

The goal is acceptable risk

© Hoyt L. Kesterson II, Slide 111 hoytkesterson@earthlink.net



?

© Hoyt L. Kesterson II, Slide 112

hoytkesterson@earthlink.net